Novell Identity Manager

3.5.1

www.novell.com

安装指南

2007 年 9 月 28 日

Novell®

法律声明

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

*联机文档：*要访问本产品及其他 Novell 产品的最新联机文档，请参阅 Novell 文档万维网页面 (http://www.novell.com/documentation)。

Novell 商标

有关 Novell 商标，请参见 Novell 商标和服务标记列表 (http://www.novell.com/company/legal/trademarks/tmlist.html)。

第三方资料

所有第三方商标均属其各自所有者的财产。

目录

关于本指南 9

1 概述 11

1.1 Identity Manager 简介 . . . 11
1.2 术语更改 . . . 13
1.3 Identity Manager 3.5.1 有哪些新功能？ . . . 14
1.3.1 Identity Manager . . . 14
1.3.2 Designer for Identity Manager . . . 15
1.3.3 User Application . . . 16
1.4 Identity Manager 安装程序和服务 . . . 18
1.4.1 安装程序 . . . 18
1.4.2 服务 . . . 20
1.5 Identity Manager 的系统要求 . . . 27
1.6 建议的部署策略 . . . 33
1.7 从何处获取 Identity Manager 及其服务 . . . 35
1.7.1 安装 Identity Manager 3.5.1 . . . 36
1.7.2 激活 Identity Manager 3.5.1 产品 . . . 37

2 计划 39

2.1 计划 Identity Manager 实施的项目管理方面 . . . 39
2.1.1 Novell Identity Manager 部署 . . . 39
2.2 常用安装场景的规划 . . . 45
2.2.1 Identity Manager 的全新安装 . . . 45
2.2.2 在同一环境中使用 Identity Manager 和 DirXML 1.1a . . . 47
2.2.3 从 Starter Pack 升级为 Identity Manager . . . 49
2.2.4 从 Password Synchronization 1.0 升级为 Identity Manager 口令同步 . . . 50
2.3 计划 Identity Manager 实施的技术方面 . . . 52
2.3.1 使用 Designer . . . 52
2.3.2 在服务器上复制 Identity Manager 需要的对象 . . . 52
2.3.3 使用 “范围过滤”管理不同服务器上的用户 . . . 53

3 升级 57

3.1 升级路径 . . . 57
3.2 策略体系结构的更改 . . . 57
3.3 升级过程 . . . 58
3.3.1 导出驱动程序 . . . 58
3.3.2 校验最低要求 . . . 59
3.3.3 升级引擎 . . . 59
3.3.4 升级 Remote Loader . . . 60
3.3.5 UNIX/Linux 环境中的升级 . . . 60
3.4 升级口令同步 . . . 60
3.5 从 RNS 升级到 Novell Audit . . . 61
3.6 升级 DirXML 1.1a 驱动程序配置 . . . 61
3.7 激活 Identity Manager . . . 61

4 安装 Identity Manager 63

4.1 安装前 . . . 63
4.2 Identity Manager 组件和系统要求 . . . 63
4.3 在 NetWare 上安装 Identity Manager . . . 63
4.4 在 Windows 上安装 Identity Manager . . . 69
4.5 在 Windows 上安装已连接系统选项 . . . 75
4.6 在 UNIX/Linux 平台上通过 GUI 界面安装 Identity Manager . . . 79
4.7 在 UNIX/Linux 平台上使用控制台安装 Identity Manager . . . 83
4.8 在 UNIX/Linux 上使用控制台安装已连接系统选项 . . . 86
4.9 Identity Manager 的非根安装 . . . 88
4.10 安装后的任务 . . . 91
4.11 安装自定义驱动程序 . . . 91

5 安装 User Application 93

5.1 安装的前提条件。. . . 93
5.1.1 安装 JBoss 应用程序服务器和 MySQL 数据库 . . . 95
5.1.2 安装 JBoss 应用程序服务器作为一项服务 . . . 97
5.1.3 配置 MySQL 数据库. . . 98
5.2 安装和配置 . . . 99
5.3 创建 User Application 驱动程序. . . 100
5.4 关于安装程序 . . . 104
5.4.1 安装底稿和可执行文件 . . . 104
5.4.2 安装时要求的值 . . . 105
5.5 在 JBoss 应用程序服务器上从安装 GUI 安装 User Application . . . 105
5.5.1 运行安装程序 GUI . . . 106
5.5.2 选择应用程序服务器平台 . . . 108
5.5.3 迁移数据库 . . . 108
5.5.4 指定 WAR 的位置. . . 110
5.5.5 选择安装文件夹 . . . 110
5.5.6 选择数据库平台 . . . 112
5.5.7 指定数据库主机和端口 . . . 114
5.5.8 指定数据库名称和特权用户 . . . 115
5.5.9 指定 Java 根目录 . . . 116
5.5.10 指定 JBoss 应用程序服务器设置 . . . 116
5.5.11 选择应用程序服务器配置类型 . . . 118
5.5.12 启用 Novell Audit 日志记录. . . 119
5.5.13 指定主密钥 . . . 119
5.5.14 配置 User Application. . . 121
5.5.15 校验选择并安装 . . . 132
5.5.16 查看日志文件 . . . 132
5.6 在 WebSphere 应用程序服务器上安装 User Application . . . 132
5.6.1 起动安装程序 GUI . . . 133
5.6.2 选择应用程序服务器平台 . . . 134
5.6.3 指定 WAR 的位置. . . 135
5.6.4 选择安装文件夹 . . . 137
5.6.5 选择数据库平台 . . . 138
5.6.6 指定 Java 根目录 . . . 140
5.6.7 启用 Novell Audit 日志记录. . . 141
5.6.8 指定主密钥 . . . 142
5.6.9 配置 User Application. . . 144
5.6.10 校验选择并安装 . . . 154
5.6.11 查看日志文件 . . . 155
5.6.12 添加 User Application 配置文件和 JVM 系统属性 . . . 155
5.6.13 将 eDirectory 可信根导入 WebSphere 密钥存储区. . . 156

5.6.14 部署 IDM WAR 文件 . . . 157
5.6.15 启动应用程序 . . . 157
5.6.16 访问 User Application 门户 . . . 157
5.7 从控制台界面安装 User Application . . . 158
5.8 使用单个命令安装 User Application . . . 158
5.9 安装后的任务 . . . 163
5.9.1 记录主密钥 . . . 163
5.9.2 检查群集安装 . . . 164
5.9.3 配置 JBoss 服务器之间的 SSL 通讯 . . . 164
5.9.4 访问外部口令 WAR . . . 164
5.9.5 升级忘记口令设置 . . . 165
5.9.6 设置电子邮件通知 . . . 165
5.9.7 在 JBoss 应用程序服务器上测试安装. . . . 165
5.9.8 设置供应小组和请求 . . . 166
5.9.9 在 eDirectory 中创建索引 . . . 166
5.10 安装后重新配置 IDM WAR 文件。 . . . 167
5.11 查错 . . . 167

6 激活 Novell Identity Manager 产品 169

6.1 购买 Identity Manager 产品许可证 . . . 169
6.2 通过使用身份凭证激活 Identity Manager 产品 . . . 169
6.3 安装产品激活身份凭证 . . . 171
6.4 查看 Identity Manager 和驱动程序的产品激活 . . . 172

关于本指南

Novell® Identity Manager （以前称为 DirXML®）是一种数据共享和同步服务，应用程序、目录和数据库可以使用它来共享信息。它链接分散的信息；发生身份更改后，还可以使用它来建立策略，用于控制对指定系统的自动更新。Identity Manager 为帐户供应、安全性、一次签到、用户自助服务、鉴定、授权、自动工作流程和万维网服务提供了基础。通过它可以集成、管理和控制分发的身份信息，以便安全地将适当的资源递送给适当的人员。

本指南概述了 Identity Manager 技术，同时介绍了 Identity Manager 的安装、管理和配置功能。

- 第 1 章 "概述"（第 11 页）
- 第 2 章 "计划"（第 39 页）
- 第 3 章 "升级"（第 57 页）
- 第 4 章 "安装 Identity Manager"（第 63 页）
- 第 5 章 "安装 User Application"（第 93 页）
- 第 6 章 "激活 Novell Identity Manager 产品"（第 169 页）

读者

本指南面向规划 Identity Manager 并将其实施到网络环境中的管理员、顾问和网络工程师。

文档更新

有关本文档的最新版本，请访问 Identity Manager 文档万维网站点 (http://www.novell.com/documentation/idm35/index.html)。

其他文档

有关其他 Identity Manager 驱动程序的文档的信息，请参见 Identity Manager 驱动程序万维网站点 (http://www.novell.com/documentation/idm35drivers/index.html)。

文档约定

在 Novell 文档中，大于号 (>) 用于分隔步骤内的操作和交叉参照路径中的项目。

商标符号 （®、™ 等）表示 Novell 商标。星号 (*) 表示第三方商标。

在书写单一路径名时，一些平台使用反斜杠而另一些平台使用正斜杠，但在本文档中路径名一律使用反斜杠表示。对于要求使用正斜杠的平台 （例如， Linux* 或 UNIX*），用户应根据软件的要求使用正斜杠。

概述 1

- 第 1.1 节 “Identity Manager 简介”（第 11 页）
- 第 1.2 节 “术语更改”（第 13 页）
- 第 1.3 节 “Identity Manager 3.5.1 有哪些新功能？”（第 14 页）
- 第 1.4 节 “Identity Manager 安装程序和服务”（第 18 页）
- 第 1.5 节 “Identity Manager 的系统要求”（第 27 页）
- 第 1.6 节 “建议的部署策略”（第 33 页）
- 第 1.7 节 “从何处获取 Identity Manager 及其服务”（第 35 页）

1.1 Identity Manager 简介

Novell® Identity Manager 是享有盛誉的数据共享和同步解决方案，它革新了数据的管理方式。该服务利用集中式数据储存 （即身份库）在应用程序、数据库和目录之间同步、转换和分发信息。

然而， Identity Manager 还有更多功能。 Identity Manager 的部分功能包括：

- 口令同步
- 口令自助服务
- 记录和审计服务
- 通过 User Application 进行用户管理
- 工作流程供应
- 电子邮件通知
- 通过 Designer 实用程序设计驱动程序和策略

要查看本版本的 Identity Manager 中有关这些组件的新增内容，请参见第 1.3 节 “Identity Manager 3.5.1 有哪些新功能？”（第 14 页）。为了更清楚地了解 Identity Manager 包含的不同组件和服务，请参见第 1.4 节 “Identity Manager 安装程序和服务”（第 18 页）。

通过 Identity Manager，已连接系统 （比如 SAP*、 PeopleSoft*、 Lotus* Notes*、 Microsoft* Exchange、 Active Directory* 等）可实现以下功能：

- 与身份库 共享数据。
- 在已连接系统中修改共享的数据后，与身份库 同步和转换此数据。
- 在身份库 中修改共享的数据后，与已连接系统同步和转换此数据。

Identity Manager 通过提供一个双向框架来实现此功能，管理员可以使用该框架指定哪些数据从身份库 流向应用程序，以及哪些数据从应用程序流向身份库。该框架使用 XML 来提供数据和事件转换功能，将身份库 数据和事件转换为指定应用程序的特定格式。它还将特定于应用程序的格式转换为身份库 可识别的格式。与应用程序的所有交互都是使用该应用程序的本机 API 进行的。

使用 Identity Manager 可以只选择与特定于已连接系统的相关记录和字段相对应的属性和类。例如，目录数据存储区可以选择与人力资源数据存储区共享用户对象，但不共享网络资

源对象 （例如服务器、打印机和卷）。反过来，人力资源数据存储区可以与其他人员共享用户的姓名、姓名缩写、电话号码和工作地点，但不共享用户的其他个人信息 （比如家庭信息和工作简历）。

如果身份库中没有用于要与其他应用程序共享的数据的类或属性，则可以通过扩展 eDirectory™ 纲要将其加入。在这种情况下，身份库 就成为一个信息储存库，它存储自身不需要、但可以供其他应用程序使用的信息。特定于应用程序的数据存储区只维护应用程序所需信息的储存库。

Identity Manager 可以完成下列任务：

- 使用事件截获身份库 中发生的更改。
- 如同集线器那样将所有数据集中在一起，从而实现数据管理的集中或分发。
- 以 XML 格式显示目录数据，以便 XML 应用程序或通过 Identity Manager 集成的应用程序可以使用和共享这些数据。
- 请精心维护身份库 对象与其他所有集成系统内的对象之间的关联，以确保所有已连接系统能够适当地反映数据发生的更改。

策略是同步数据的关键所在。策略：

- 使用特定过滤器来管理系统中定义的数据要素，从而控制数据流。
- 使用许可权限和过滤器实施授权数据源。
- 将规则应用到采用 XML 格式的数据存储区数据。当更改流经 Identity Manager 时，这些规则将会控制数据的解释和转换。
- 将数据从 XML 格式转换为几乎任何一种数据格式。这使 Identity Manager 能够与任何应用程序共享数据。

使用 Identity Manager，企业可以简化 HR 过程、减少数据管理成本、通过高度自定义化的服务建立客户关系并消除迈向成功过程中的协作障碍。下面是通过 Identity Manager 实施的某些示例活动：

表 1-1 *Identity Manager 的功能*

活动	Identity Manager 解决方案
管理用户帐户	通过单一操作： Identity Manager 立即授予或去除员工对资源的访问权限。 Identity Manager 提供自动化的员工供应功能，可以指定新员工对网络、电子邮件、应用程序、资源等的访问权限。通过工作流程供应，可以设置该进程以启动批准处理。 Identity Manager 还可以针对辞职或离职限制或禁用访问权限。
跟踪和集成资产库存	Identity Manager 可以将所有资产库存项目 （计算机、监视器、电话、库资源、椅子、桌子等）的配置文件添加到身份库，并将这些配置文件与个人、部门或组织等用户配置文件集成。
自动创建白页 / 黄页目录	Identity Manager 可以使用不同的信息级别创建统一的目录，以供内部和外部使用。外部目录可能只包括电子邮件地址；内部目录可能包括位置、电话号码、传真号码、手机号码、住宅地址等等。

活动	**Identity Manager 解决方案**
增强用户配置文件	Identity Manager 通过添加或同步电子邮件地址、电话号码、住宅地址、喜好、报告关系、硬件资产、电话、钥匙、库存等信息来增加用户配置文件。
统一通讯访问权限	Identity Manager 可以简化各个用户或组的网络、电话、寻呼机、万维网或无线访问权限，方法是将每种通讯的目录同步到一个通用的管理界面。
加强合作伙伴关系	Identity Manager 可以加强合作伙伴关系，方法是在防火墙以外的合作伙伴系统中创建配置文件 （员工、客户等），使合作伙伴能够按需提供即时服务。
改善供应链	Identity Manager 可通过识别和合并每个客户的多个帐户的实例来改善客户服务。
建立客户忠诚度	Identity Manager 在识别客户需求方面提供了新的服务，可以在一个位置查看数据，而不是将数据分隔在不同的应用程序或区域中。
自定义服务	Identity Manager 可以为用户 （员工、客户、合作伙伴等）提供使用已同步信息 （包括关系、状态和服务记录）完成的配置文件。 这些配置文件可用于提供对服务和信息的不同级别的访问权限，以及根据客户的信誉提供实时和自定义的服务。
口令管理	通过 User Application，管理员可以设置询问响应问题，还允许用户设置他们自己的口令。 Client Login Extension for Novell Identity Manager 3.5.1 通过添加 Novell 和 Microsoft GINA 登录客户程序的链接，简化了口令自助服务。通过这两个客户程序，可以访问 Identity Manager User Application 口令自助服务功能。 如果 Identity Manager 驱动程序支持口令同步，则口令可以在所有已连接系统上同步。

1.2 术语更改

下列术语与早期版本中的术语有所不同：

表 1-2 术语更改

早期版本中的术语	新术语
DirXML®	Identity Manager
DirXML 服务器	元目录服务器
DirXML 引擎	元目录引擎
eDirectory™	身份库 （指 eDirectory 属性或类时除外）

1.3 Identity Manager 3.5.1 有哪些新功能？

- 第 1.3.1 节 “Identity Manager”（第 14 页）
- 第 1.3.2 节 “Designer for Identity Manager”（第 15 页）
- 第 1.3.3 节 “User Application”（第 16 页）

1.3.1 Identity Manager

- 支持 Open Enterprise Server 2 （第 14 页）
- iManager 插件 （第 14 页）
- 其他操作系统平台支持 （第 14 页）
- 其他应用程序支持 （第 14 页）
- 非根安装 （第 14 页）
- 捆绑组件 （第 14 页）

支持 Open Enterprise Server 2

Open Enterprise Server 2 包含许多必备软件组件，包括 SUSE® Linux Enterprise Server 10 Support Pack 1、NetWare® 6.5 Support Pack 7、eDirectory 8.8 Support Pack 2、iManager 2.7 和 Security Services 2.0.5。 Identity Manager 在 Linux 和 NetWare Open Enterprise Server 2 平台上都受支持。

iManager 插件

此版本 Identity Manager 中的 iManager 插件也兼容 Identity Manager 3.0。除向后兼容性外， Identity Manager 3.5.1 还包含一些插件，可报告驱动程序超速缓存文件中的信息。

其他操作系统平台支持

Identity Manager 可支持先前版本 Identity Manager 支持的所有操作系统平台。此外， Identity Manager 的某些组件可运行在 Microsoft Windows Vista*、 AIX* 5.3、 Red Hat* 5 AS/ES 64-bit 和 Open Enterprise Server 2（包括 SUSE Linux Enterprise Server 10 SP1 和 NetWare 6.5 SP7）。

其他应用程序支持

Identity Manager 可支持先前版本 identity manager 支持的所有应用程序。此外，在运行有这些应用程序的平台上， Identity Manager 还支持 eDirectory 8.8 SP2 和 iManager 2.7。

非根安装

Identity Manager 3.5.1 包括将 Identity Manager 元目录引擎安装到非根安装的 eDirectory 中的信息和底稿。有关执行 Identity Manager 非根安装的步骤，请参见第 4.9 节 “Identity Manager 的非根安装”（第 88 页）。

捆绑组件

Identity Manager 包括 Client Login Extension for Novell Identity Manager 3.5.1 和 Designer 2.1。

Client Login Extension for Novell Identity Manager 3.5.1 是 Identity Manager 的新组件，通过添加 Novell 和 Microsoft GINA 登录客户程序的链接，简化了口令自助服务。当用户单击其登录客户程序中的*忘记口令*链接时， Client Login Extension 会起动内部浏览器访问 Identity Manager User Application 口令自助服务功能。此功能有助于减少由于人们忘记口令而打电话给 Help Desk 的次数。

有关 Client Login Extension for Novell Identity Manager 3.5.1 的更多信息，请参见 《*Novell Identity Manager 3.5.1 管理指南*》中的 "Client Login Extension for Novell Identity Manager 3.5.1"。有关 Designer 2.1 的更多信息，请参见第 1.3.2 节 "Designer for Identity Manager" （第 15 页）。

1.3.2 Designer for Identity Manager

本部分说明了 Designer for Identity Manager 的增强功能。有关所有 Designer 2.1 增强功能和更改的更详细列表，请参见新增内容 (http://www.novell.com/documentation/designer21/index.html)。

- 区域设置支持 （第 15 页）
- 供应小组编辑器 （第 15 页）
- "供应"视图可用性增强功能 （第 15 页）
- 电子邮件活动 （第 16 页）
- 批准活动 （第 16 页）
- 日志活动 （第 16 页）
- 表单增强功能 （第 16 页）
- ECMA 增强功能 （第 16 页）
- 供应请求定义显示名称的增强功能 （第 16 页）

区域设置支持

现在，通过 Designer for Identity Manager 的 "供应"视图，可以定义：

- User Application 的默认区域设置。（这是在无法找到匹配的用户区域设置时用于显示内容的区域设置。）
- User Application 驱动程序支持的区域设置。

此外，现在 Designer 可以导入及导出本地化数据，用于电子邮件模板。

供应小组编辑器

现在， Designer for Identity Manager 包括一个供应小组编辑器插件。通过此新编辑器，您可以定义一组用户，这些用户可以作为 User Application *请求及批准*选项卡上的一组。小组定义决定可以管理该小组相关的供应请求及批准任务的用户。

供应小组编辑器还提供了替代 iManager 插件进行小组管理的组件。

"供应"视图可用性增强功能

增强了 "供应"视图，因此您现在能够执行以下操作：

- 按类别组织供应请求定义。您可以使用目录抽象层编辑器定义类别。

- 一次为多个供应请求定义指派多个属性 （例如，受托者指派）。

电子邮件活动

电子邮件活动提供了一种方式，可向批准活动外的感兴趣各方发送电子邮件。

批准活动

现在，批准活动提供了一种方式，可从批准活动属性页创建新表单。

通过批准活动还可以在电子邮件通知中设置与 “发件人”地址不同的 “回复”地址字段。

日志活动

现在，日志活动允许向工作流程的注释历史添加自定义讯息。

表单增强功能

现在，表单支持 onload 事件。

ECMA 增强功能

以下字段方法现在都受支持：

- getName()
- validate()
- hide()
- show()
- focus()
- select()
- activate()
- setRequired()

供应请求定义显示名称的增强功能

现在，供应请求定义的显示名称可以定义为静态字符串或可本地化的 ECMA 表达式。通过定义表达式，可以自定义批准任务显示名称。这使同一工作流程的不同实例在 User Application 的任务列表中可显示为唯一项。

1.3.3 User Application

- 用户界面增强功能 （第 17 页）
- 跨平台更改 （第 17 页）
- 互操作性更改 （第 17 页）
- SOAP 端点增强功能 （第 17 页）
- 其他功能增强 （第 18 页）

用户界面增强功能

增强了 “小组任务”的显示，以在界面中提供更大的灵活性，并优化用户体验。“小组任务”页以两种新外观视图显示动态内容，“模板”视图和 “展示”视图。这两种格式都使用表向用户显示数据。在任一格式中，用户都可以选择要显示的列，指定列的显示顺序，以及按列中的值对任务排序。

管理员控制对显示格式的选择。由于具有外观自选设置功能，管理员可以选择一个视图覆盖另一个视图，也可选择使用以下辨别功能：

- “模板”视图 （默认值）为视力不佳的用户提供了辅助功能选项支持。此外，该视图包括可自定义的寻呼功能。
- “展示”视图支持过滤，并提供数据导出工具。

跨平台更改

此发行版增加了对以下应用程序服务器平台的运行时支持：

- JBoss* 4.2.0，在 SUSE Linux Enterprise Server 10.1、 SUSE Linux Enterprise Server 9 SP2 和 Windows 2003 Server SP1 上
- WebSphere* 6.1，在 Solaris* 10 和 Windows 2003 SP1 上

  User Application 的安装程序会为您安装 WAR。但是，您需要手动将 WAR 部署到 WebSphere。

  对 WebSphere 的数据库支持包括 Oracle* 10g、 MS SQL* 2005 SP1 和 DB2。

  有关受支持平台的完整列表，请参见 Identity Manager 的系统要求 （第 27 页）。

此发行版还增加了对以下浏览器环境的支持：

- Internet Explorer 7，在 Windows 2000 Professional SP4、 Windows XP SP2 和 Windows Vista Enterprise V6 上
- Firefox* 2，在 Red Hat Enterprise Linux WS 4.0、 Novell Linux Desktop 9、 SUSE Linux 10.1 和 SUSE Linux Enterprise Desktop 10 上

互操作性更改

在此发行版中进行了以下互操作性更改：

- 现在管理员可以使用配置设置指定 User Application 是否在 “忘记口令”屏幕上显示 “提示”。
- 现在，管理员可以使用配置设置来启用或禁用 “登录”对话框中的口令自动完成功能。此功能控制浏览器是否允许用户保存他们的身份凭证。
- 现在，登录进程支持通过 Access Manager 鉴定代理智能卡。为实现此功能， User Application 接受插入到 HTTP 头的 SAML 断言，并使用这些断言生成 SASL 到目录的连接。

SOAP 端点增强功能

此发行版对 SOAP 端点增强了以下功能：

- 增加了新 VDX 服务，以提供一个 SOAP 端点用于对目录抽象层执行查询操作。
- 增加了新通知服务，以提供一个 SOAP 端点用于发送电子邮件通知。

- 供应服务增加了一个名为 getProcessesArray() 的新方法，通过该方法中的一个自变量，您可以限制返回的进程数。
- 供应服务还增加了一个名为 startWithCorrelationId() 的新方法，通过该方法，您可以开始一组相关的工作流程并使用相关性 ID 跟踪它们。

SOAP 端点为开发人员提供了用于构建他们自己的应用程序的方式。但是， User Application 的初始用户界面不显示这些方式。

其他功能增强

现在 User Application 允许您指定 URL 参数，以直接跳转到供应请求表单。

1.4 Identity Manager 安装程序和服务

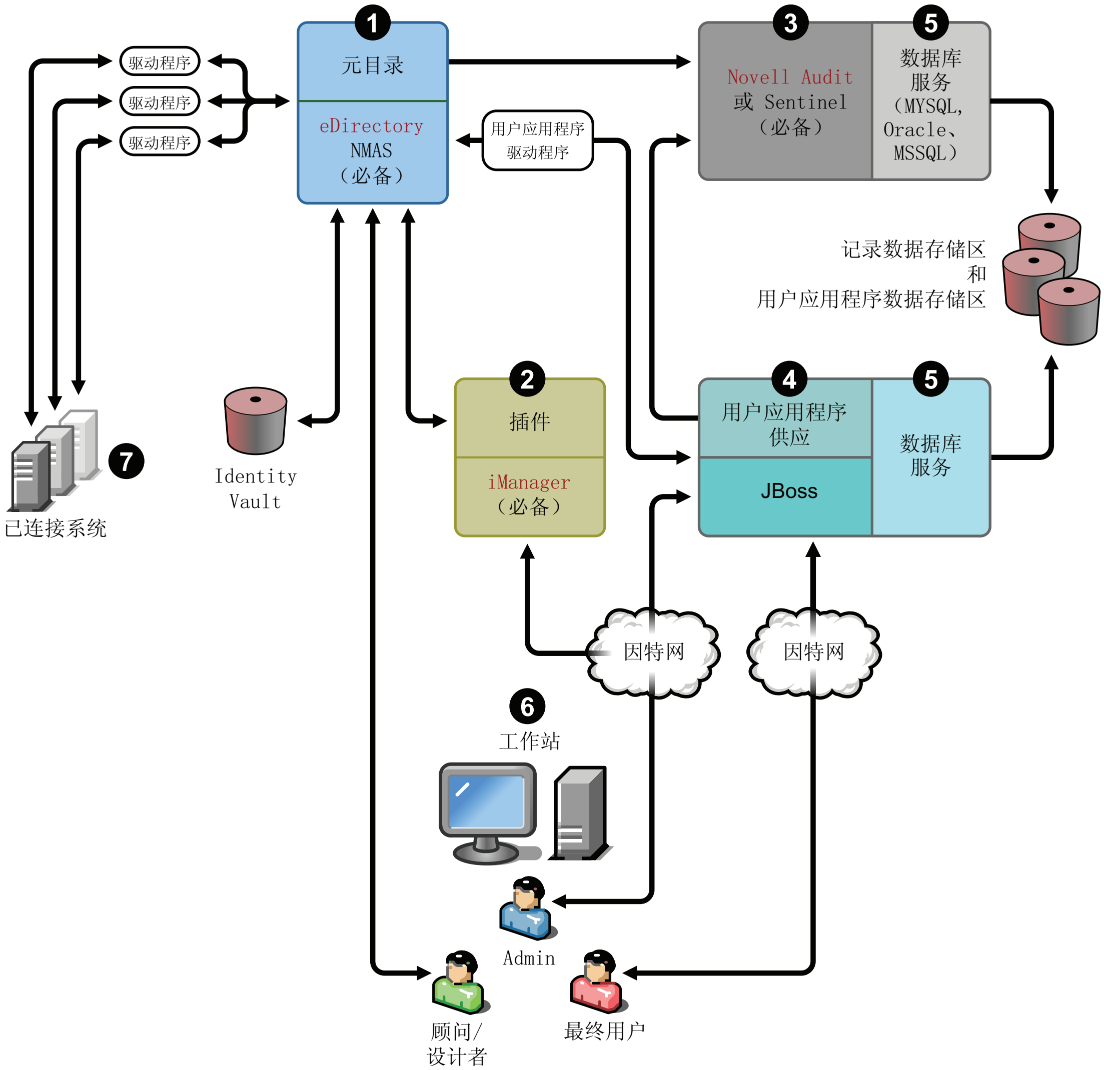
以下部分将说明 Identity Manager 的安装程序和服务。本部分说明功能完整的 Identity Manager 所包含的各种服务。

- 第 1.4.1 节 “安装程序”（第 18 页）
- 第 1.4.2 节 “服务”（第 20 页）

1.4.1 安装程序

Identity Manager 具有三个独特的安装程序，以及七项需要安装和配置的服务。通过下图，可以总体了解一个功能完整的 Identity Manager 所必需的全部服务。

图 1-1　七项 Identity Manager 服务的图形概览



下面是安装程序的列表以及每个安装过程执行的任务：

- Identity Manager 元目录系统安装 （第 20 页）
- User Application 和供应模块安装 （第 20 页）
- Designer 安装 （第 20 页）

注释：在安装 Identity manager 组件之前，需要首先安装必备软件，包括 edirectory 8.7.3.6 或更高版本 （对于上图中编号为 1 和 3 的服务）、带 NMAS™ 3.1.3 的 Security Services 2.0.4 （对于编号 1 和 3）、 iManager 2.6 或更高版本 （对于编号 2）以及 Novell Audit 2.0.2 Starter Pack 或 Sentinel™ 5.1.3 （对于编号 3）。可以从 Novell 下载万维网站点 (http://download.novell.com) 获取必备软件。有关必备软件和要求的详细列表，请参见第 1.5 节 “Identity Manager 的系统要求”（第 27 页）。

Identity Manager 元目录系统安装

安装过程执行下列功能：

- 将 Identity Manager 产品的 eDirectory 纲要作为一个整体进行扩展。
- 安装 元目录引擎和系统服务。
- 安装 iManager 的 Identity Manager 插件。
- 安装 元目录系统远程装载程序 （如果已选择）。
- 安装已连接系统驱动程序。（将会安装驱动程序，但是在启动以供使用之前，这些驱动程序将处于休眠状态）。
- 安装 Identity Manager 报告以及元目录系统实用程序和工具。

User Application 和供应模块安装

将在 Linux* 和 Windows 上安装以下服务：

- JBoss* 和 MySQL* （如果选中）。
- 运行 User Application 所需的 WAR 文件。

Designer 安装

Linux 和 Windows 各有一个安装程序。它们执行以下任务：

- 安装 Eclipse* 框架。
- 安装基本插件。
- 安装 元目录插件。
- 安装目录抽象层插件。
- 安装工作流程编辑器插件。

1.4.2 服务

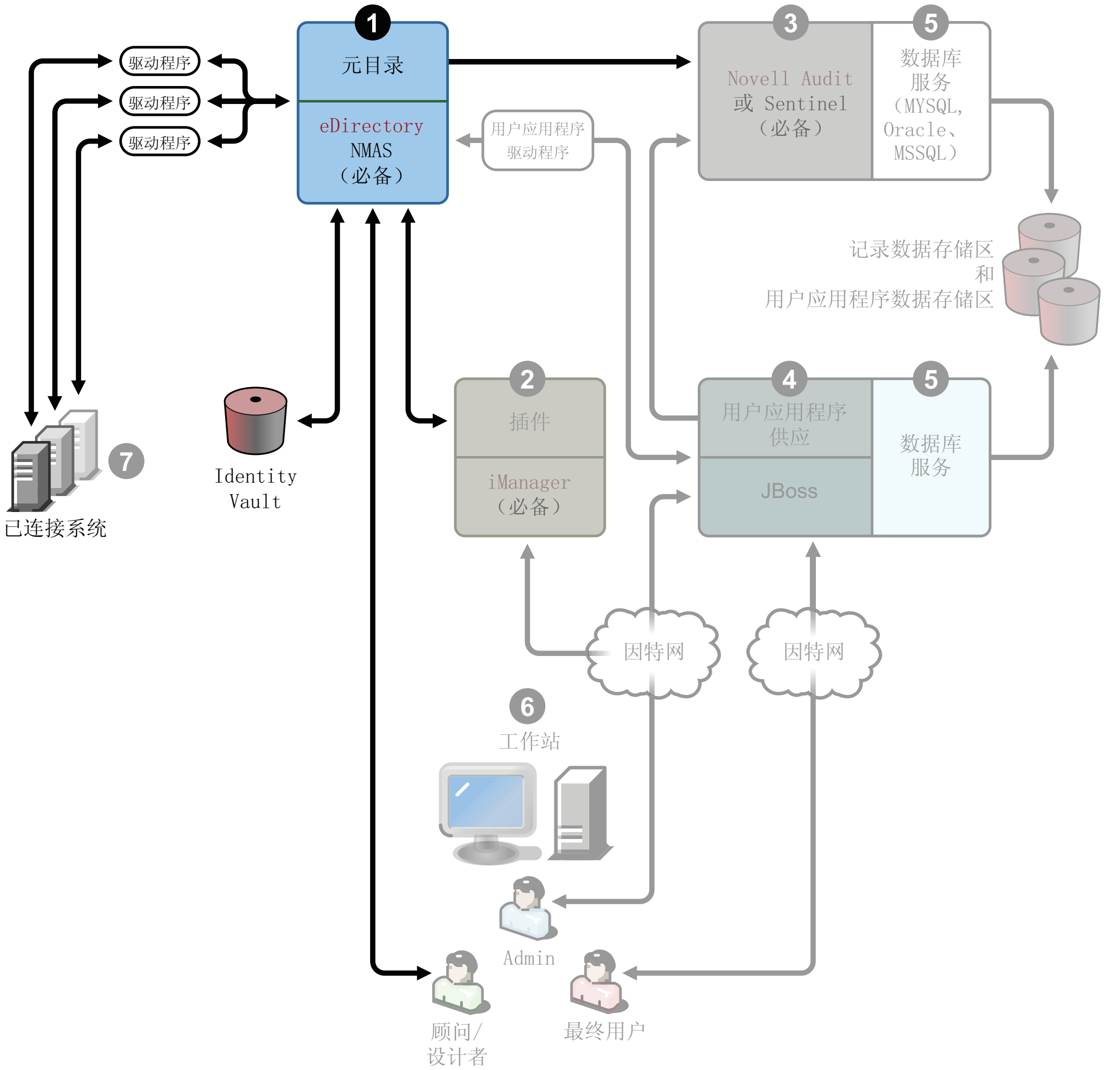
Identity Manager 附带七项可以安装和配置的服务。尽管建议不要用于生产环境，但仍可以在一台计算机上安装和配置所有七项服务。或者也可以在每台计算机上部署一至六项服务。第 1.5 节 “Identity Manager 的系统要求”（第 27 页）中包含了每项服务支持的硬件和软件必备条件。

- 元目录系统服务 （第 20 页）
- 基于万维网的管理服务 （第 22 页）
- 安全日志记录服务 （第 23 页）
- User Application 和供应模块 （第 24 页）
- 数据库服务 （第 24 页）
- 工作站 （第 26 页）
- 已连接系统 （第 26 页）

元目录系统服务

该系统将用作身份库，在生产环境中只需要 元目录引擎的一个实例。

图 1-2 元目录系统服务

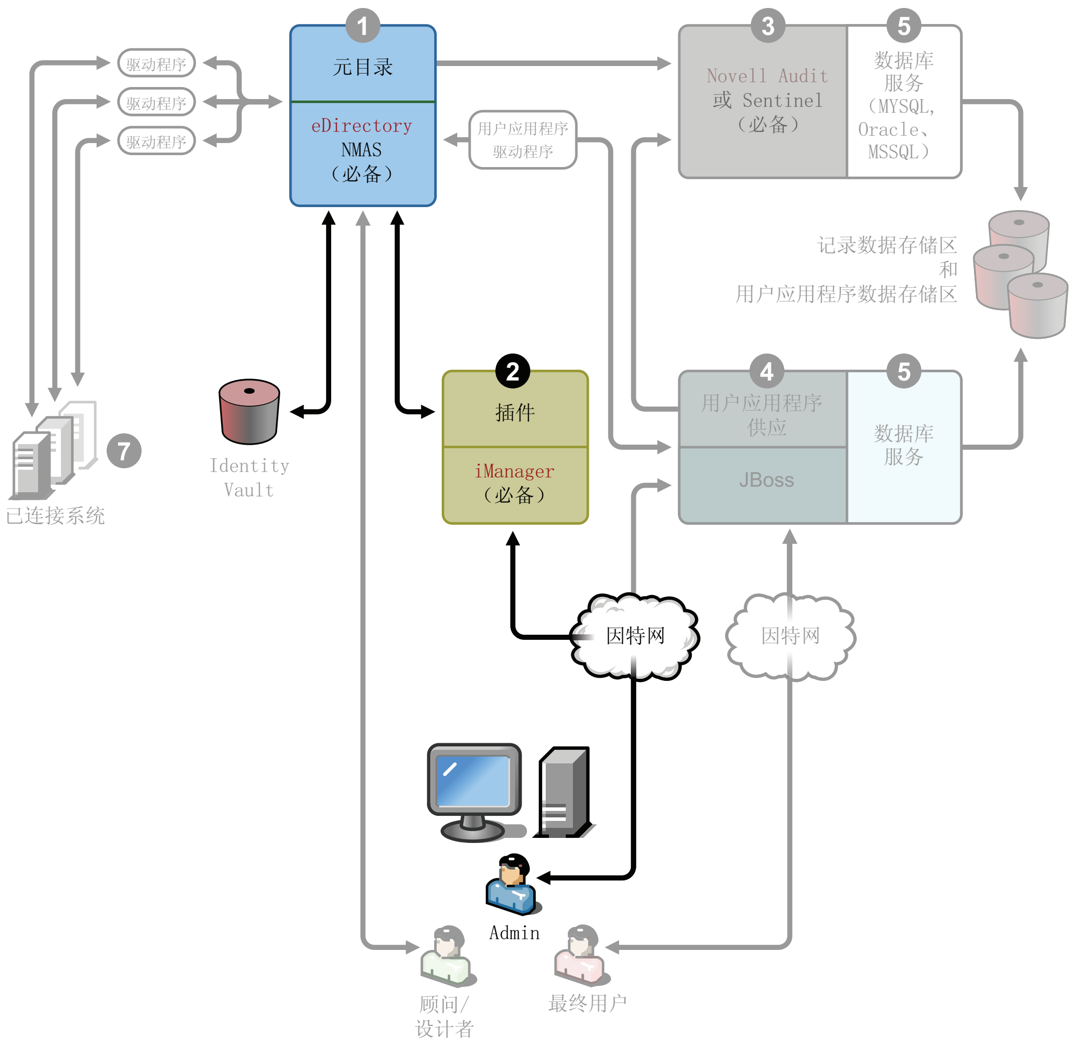


当一个系统中的数据发生变化时， Identity Manager 包含的元目录引擎将会根据定义的业务规则检测这些更改，并将这些更改传播到其他已连接系统。使用此解决方案，可对任何特定数据段强制使用授权数据源 （例如， HR 应用程序拥有用户的 ID，而讯息交换系统可能拥有用户的电子邮件帐户信息）。

要安装 Identity Manager 和该服务，请参见第 4 章 “安装 Identity Manager”（第 63 页）。要在安装 Identity Manager 之前查看先决条件，请参见对于元目录系统 （第 28 页）的系统要求。

基于万维网的管理服务

图 1-3 基于万维网的管理服务



在安装了 Identity Manager 和 User Application 插件的情况下，可使用该服务来管理使用 iManager 2.5 及更高版本的 eDirectory 和元目录系统。可以将 Identity Manager 插件安装到 Identity Manager 所在服务器上的 iManager 中。要安装 Identity Manager 插件和该服务，请参见第 4 章 “安装 Identity Manager”（第 63 页）。

安全日志记录服务

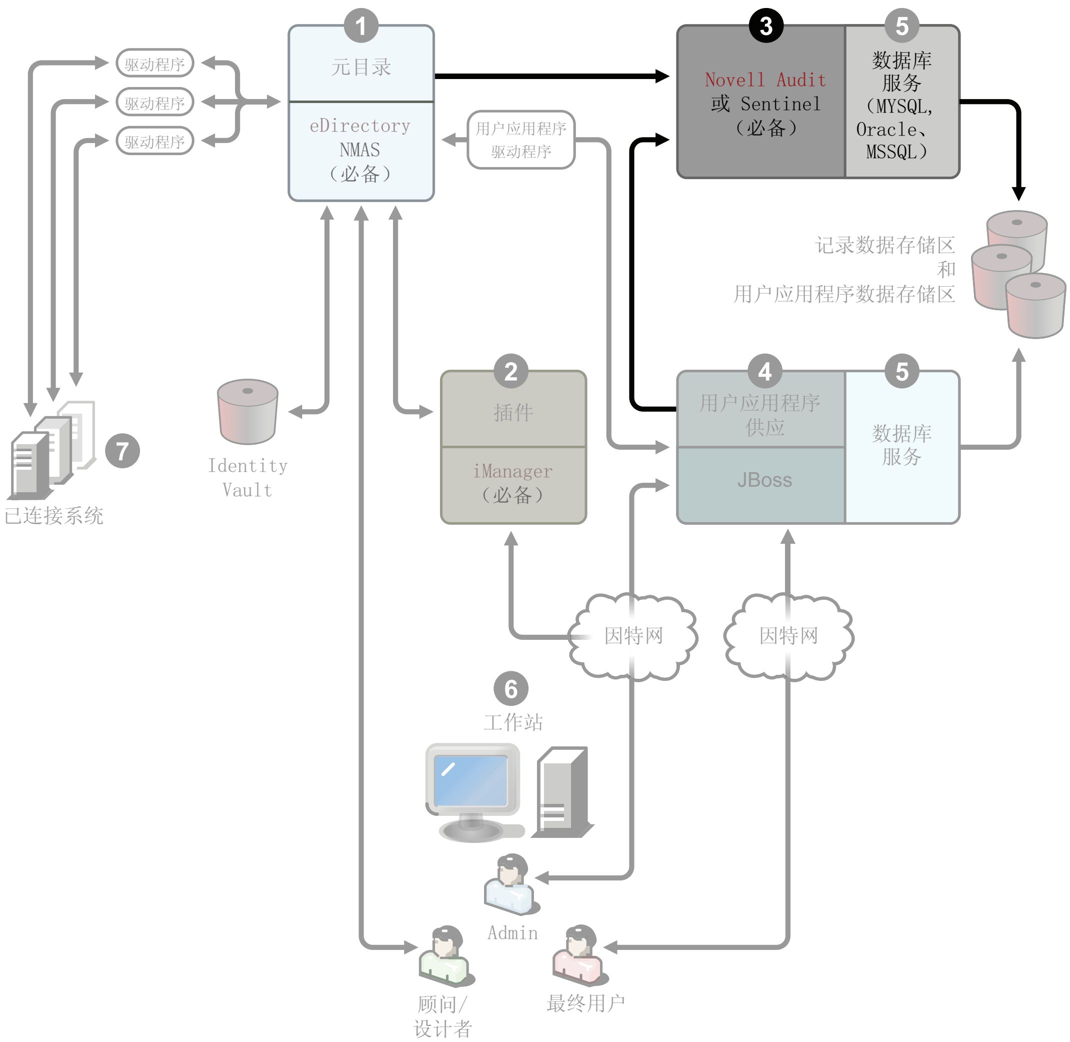


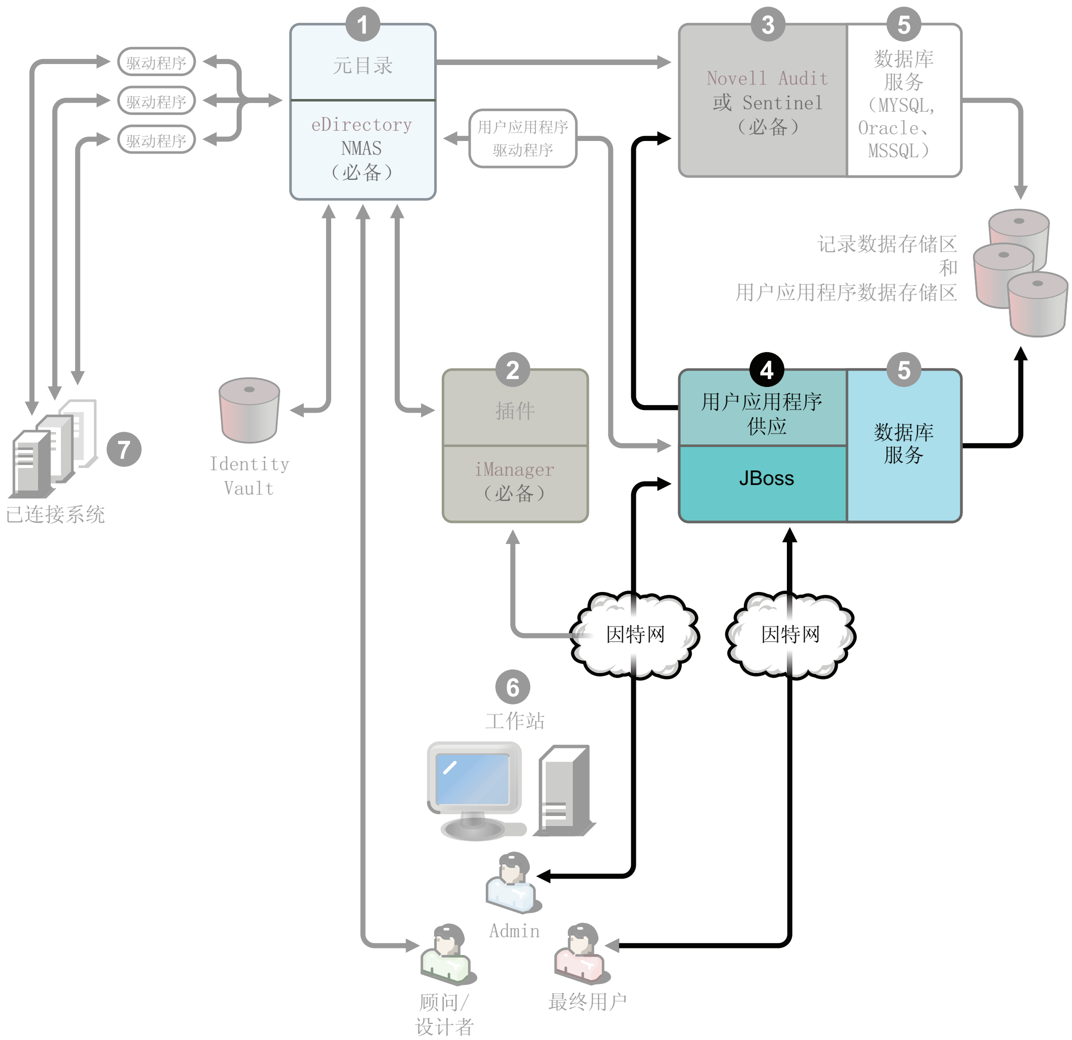
图 1-4 安全日志记录服务

日志记录事件的储存库 （此服务器上未安装 Identity Manager 软件，但必须具备安全日志记录服务）。这是由 Identity Manager、User Application 和工作流程系统服务使用的中央服务，需要从 Novell 下载万维网站点 (http://download.novell.com) 单独下载该服务。

在下载万维网站点上的*产品或技术*下拉菜单中，选择 *Audit*，然后单击*搜索*。单击 *Audit 2.0.2 Starter Pack*。遵循 Starter Pack 包含的安装指导。

User Application 和供应模块

图 1-5 User Application 和供应模块

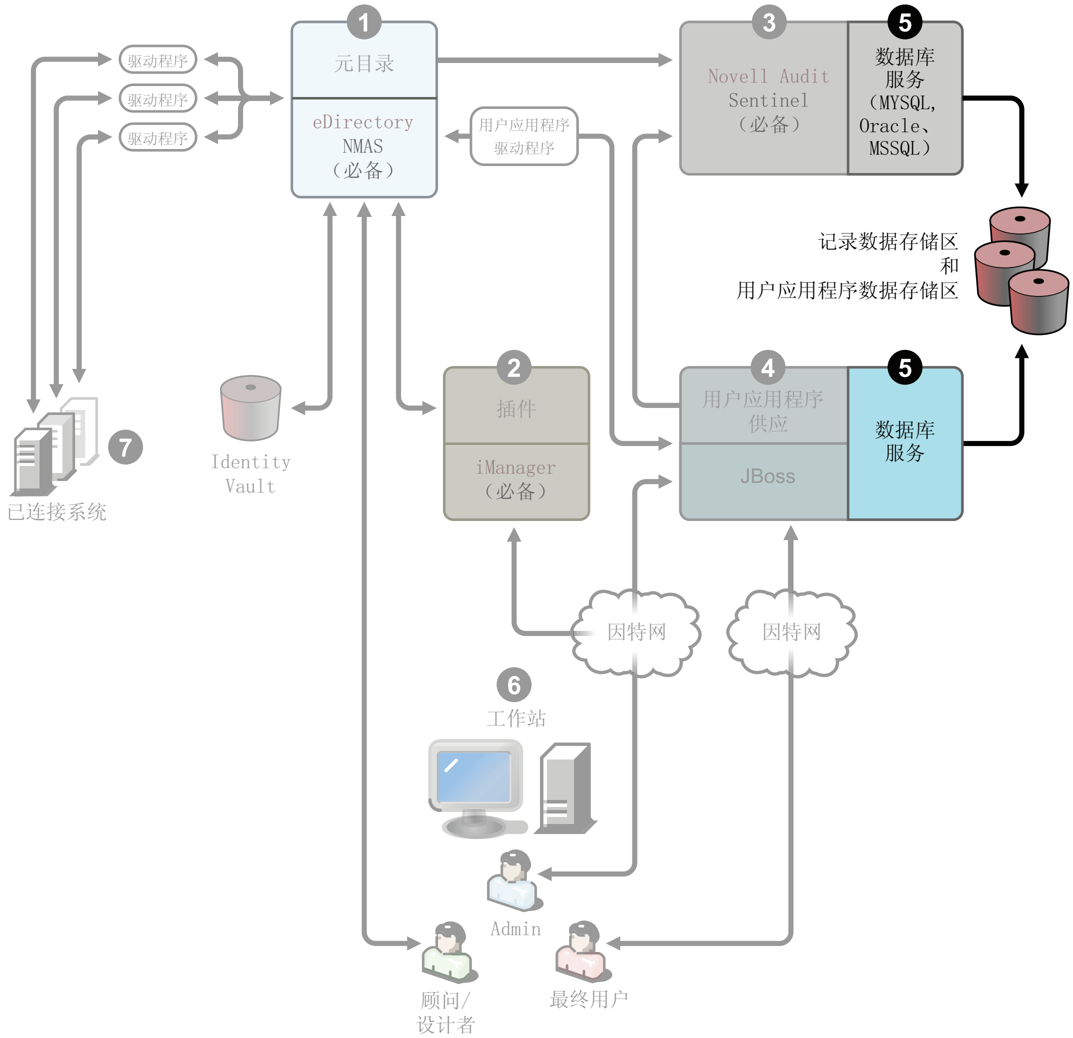


要安装该服务，请参见第 5 章 “安装 User Application”（第 93 页）。第 5.1 节 “安装的前提条件。”（第 93 页）中包含了每个服务支持的硬件和软件必备条件。

数据库服务

安全日志记录服务和最终 User Application/ 工作流程系统都需要数据库。可以设置一个数据库同时为两个应用程序提供服务，也可以为每个应用程序设置独立的数据库。

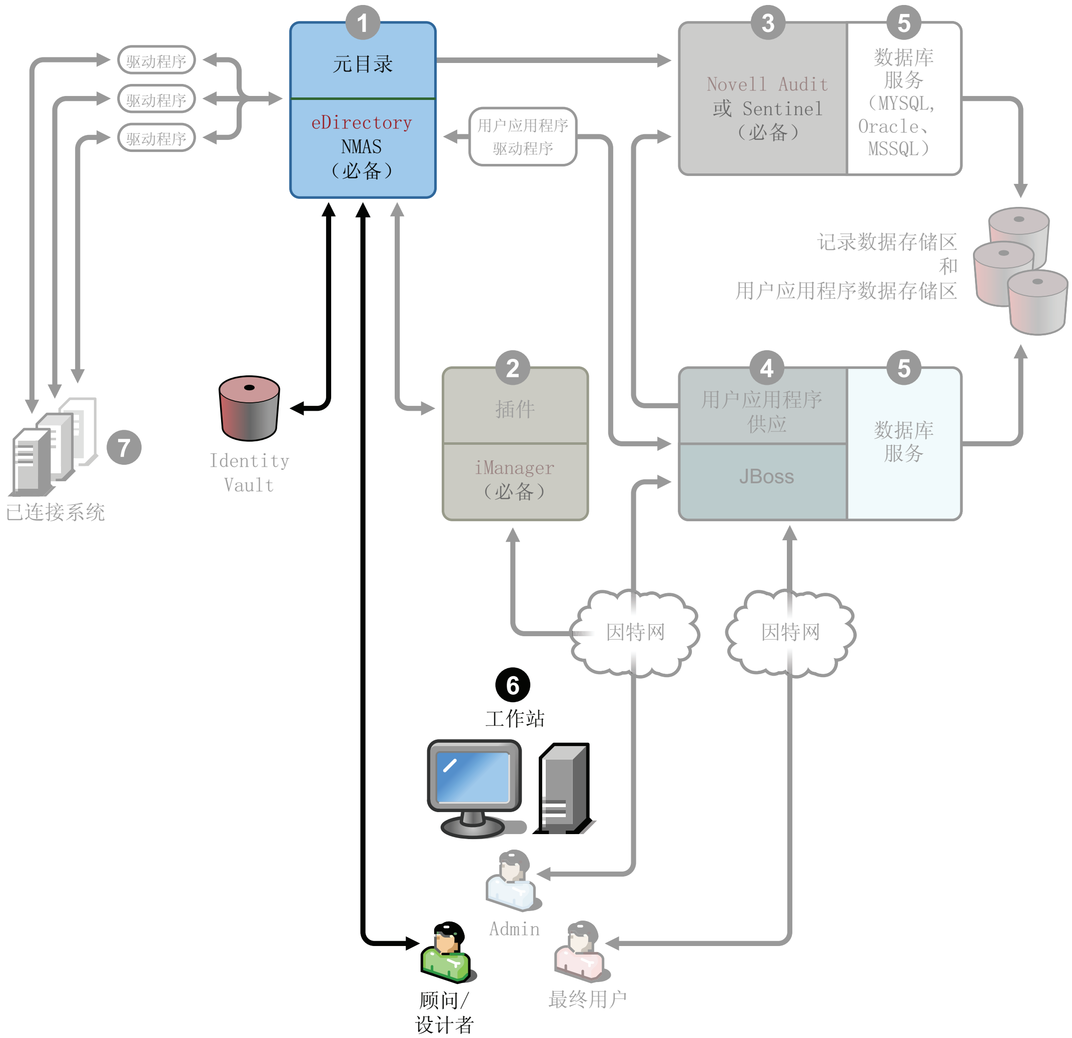
图 1-6 数据库服务



安全日志记录服务不包括特定数据库。但是，可以使用 User Application 和供应附带的 MySQL 数据库。User Application 附带有 JBoss Application Server V4.2.0，并且 User Application 需要 JRE* 1.5.0_10。要安装该服务，请参见第 5.2 节 “安装和配置”（第 99 页）。

工作站

图 1-7 Designer 的工作站服务

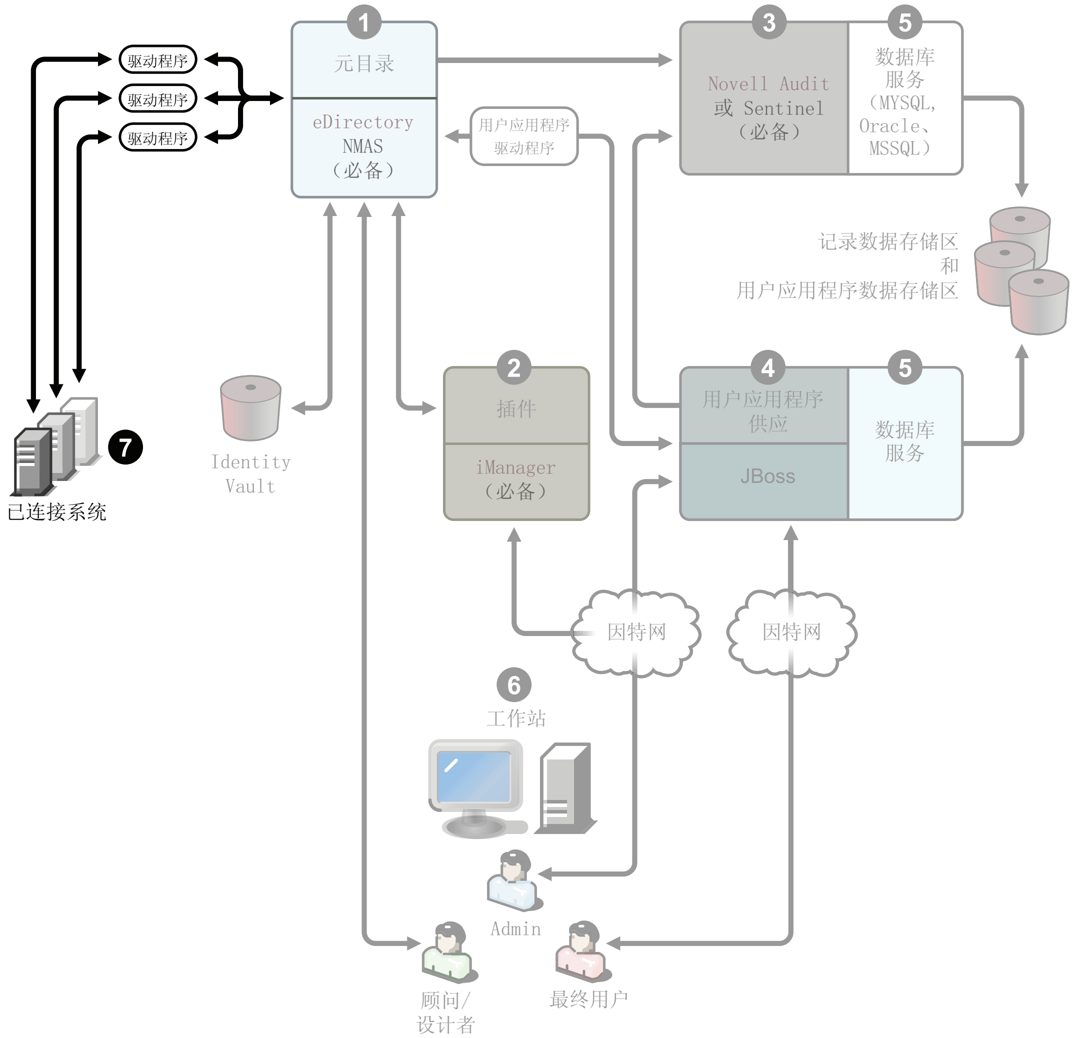


供 Designer 设计、部署和记录 Identity Manager 系统，并用于产品中包含的实用程序、报告和工具。要在工作站上安装 Designer，请参见 *Designer 2.1 for Identity Manager 3.5.1* 中的 “安装 ”。

已连接系统

这是放置驱动程序的位置，这些已连接系统可以是应用程序、数据库、服务器和其他服务。每个已连接应用程序都要求个人具有特定于应用程序的知识并承担相关责任。每个驱动程序都要求已连接系统可用并且提供了相关的 API。

图 1-8 已连接系统



驱动程序的安装是 Identity Manager 安装过程的一部分。要安装 Identity Manager 和该服务，请参见第 4 章 “安装 Identity Manager”（第 63 页）。要了解有关配置驱动程序的详细信息，请阅读 Identity Manager 驱动程序文档万维网站点 (http://www.novell.com/documentation/idmdrivers) 上特定于驱动程序的文档。

1.5 Identity Manager 的系统要求

Novell Identity Manager 中包含了可安装在多系统和多平台环境中的组件。根据系统配置的不同，可能需要多次运行 Identity Manager 安装程序，才能在相应的系统上安装 Identity Manager 组件。

下表列出了 Identity Manager 的安装组件以及每个组件的要求。

表 1-3 Identity Manager 系统组件和系统要求

系统组件	系统要求	注释
元目录系统 ◆ 元目录引擎 ◆ Novell Audit 代理 ◆ 服务驱动程序 ◆ Identity Manager 驱动程序 ◆ 实用程序 （包括应用程序工具和 Novell Audit 设置工具）	下列操作系统之一： ◆ 带最新 Support Pack 的 NetWare 6.5 ◆ 带最新 Support Pack 的 Novell Open Enterprise Server (OES) 1.0 ◆ Novell Open Enterprise Server (OES) 2.0 ◆ 带最新 Service Pack 的 Windows 2000 Server （32 位） ◆ 带最新 Service Pack 的 Windows Server 2003 （32 位） ◆ Linux Red Hat 3.0、 4.0 和 5.0 ES 和 AS （同时支持 32 位和 64 位） ◆ 带最新 Support Pack 的 SUSE Linux Enterprise Server 9 和 10 （同时支持 32 位和 64 位） ◆ Solaris 9 或 10 ◆ AIX 5.2L， V5.2 和 5.3 下列 eDirectory 版本之一： ◆ 带最新 Support Pack 的 eDirectory 8.7.3.6 ◆ 带最新 Support Pack 的 eDirectory 8.8 Security Services 2.0.5 (NMAS 3.1.3)	如果使用 元目录系统平台，则支持在实施中使用 VMWare*。 此发行版中的所有 Identity Manager 软件组件都为 32 位，即使它们在 64 位处理器或 64 位操作系统上运行。除非另行指定，否则 OES、 NetWare、 Windows 和 Linux 平台 （Red Hat 和 SUSE）支持下列所有 32 位模式的处理器： ◆ Intel* x86-32 ◆ AMD x86-32 ◆ Intel EM64T ◆ AMD Athlon64* 和 Opteron* Identity Manager 支持 eDirectory 8.8 的以下功能： ◆ 同一服务器上的多个 eDirectory 实例 ◆ 加密的属性 eDirectory 8.8 支持 64 位 Red Hat Linux 4.0。 可提供 Windows Server 2003 上的 64 位版的口令同步。 安装 eDirectory 8.8 之前，请务必完全备份 eDirectory 数据库。 eDirectory 8.8 将会升级数据库结构的某些部分，并且在完成升级过程后不允许数据库结构回滚。 在超虚拟化模式下，当 Xen Virtual Machine (VM) 运行 SLES 10 以作为 guest 操作系统时， SUSE Linux Enterprise Server 10 上现在支持 Xen 虚拟化。需要针对 SLES 10 的 Xen 增补程序（请参见 TID # 3915180 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3915180&sliceId=SAL_Public&dialogID=20406933&stateId=0%200%2020414606)）。

系统组件	系统要求	注释
基于万维网的管理服务器 ◆ 口令同步 ◆ iManager 2.6 和插件 ◆ iManager 2.7 和插件 ◆ 驱动程序配置	下列操作系统之一： ◆ 带最新 Support Pack 的 NetWare 平台上的 Novell Open Enterprise Server (OES) 1.0 ◆ Novell Open Enterprise Server (OES) 2.0 ◆ 带最新 Support Pack 的 NetWare 6.5 ◆ 带最新 Service Pack 的 Windows 2000 Server （32 位） ◆ 带最新 Service Pack 的 Windows Server 2003 （32 位） ◆ Microsoft Windows Vista ◆ Linux Red Hat 3.0、 4.0 和 5.0 ES 及 AS （同时支持 32 位和 64 位） ◆ 带最新 Support Pack 的 Solaris 9 或 10 ◆ 带最新 Support Pack 的 SUSE Linux Enterprise Server 9 和 10 （同时支持 32 位和 64 位） 通过 iManager 工作站支持操作系统： ◆ 带最新 Service Pack 的 Windows 2000 Professional ◆ 带 SP2 的 Windows XP ◆ SUSE Linux Enterprise Desktop 10 ◆ SUSE Linux 10.1 下列软件。 ◆ 带最新 Support Pack 和插件的 Novell iManager 2.6 和 2.7。	此发行版中的所有 Identity Manager 软件组件都为 32 位，即使它们在 64 位处理器或 64 位操作系统上运行。除非另有规定，否则 OES、 NetWare、 Windows 和 Linux 平台 （Red Hat 和 SUSE）支持下列所有 32 位模式的处理器： ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 和 Opteron ◆ 浏览器支持由 iManager 2.6 确定。目前该列表包括： ◆ Internet Explorer 6 SP1 和更高版本 ◆ Internet Explorer 7 ◆ Firefox* 2.0 和更高版本 ◆ 必须使用 iManager 配置向导或 Designer 实用程序将入口内容安装或部署到 eDirectory 中。 ◆ (Windows) 可以从 Novell 软件下载 (http://download.novell.com/index.jsp) 获取 Novell Client™ 4.9。 ◆ 使用 iManager 登录到其他树以管理远程 Identity Manager 服务器时，如果使用该远程服务器的名称而不是 IP 地址，则可能会遇到错误。 ◆ 口令同步代理只在 64 位 Windows 2003 上受支持。

系统组件	系统要求	注释
安全日志记录服务 ◆ 安全日志记录服务器 ◆ 平台代理 （客户机组件） ◆ Novell Audit 2.0.2 或 Sentinel 5.1.3	对于安全日志记录服务器，需要下列操作系统之一： ◆ 带最新 Support Pack 的 Novell Open Enterprise Server (OES) 1.0 和 2.0 ◆ 带最新 Support Pack 的 NetWare 6.5 ◆ 带最新 Service Pack 的 Windows 2000 Server （32 位） ◆ 带最新 Service Pack 的 Windows 2003 server （32 位） ◆ Red Hat Linux 3.0、 4.0 和 5.0 AS 和 ES （32 位和 64 位，虽然 Novell Audit 只运行于 32 位模式） ◆ 带最新 Support Pack 的 Solaris 9 或 10 ◆ SUSE Linux Enterprise Server 9 或 10 （32 位和 64 位，虽然 Novell Audit 只运行于 32 位模式） ◆ 带最新 Support Pack 的 Novell eDirectory 8.7.3.6 或 8.8 （必须安装在安全日志记录服务器上） 对于平台代理，需要下列操作系统之一： ◆ Novell Open Enterprise Server (OES) 1.0 SP1 或带最新 Support Pack ◆ 带最新 Support Pack 的 NetWare 6.5 ◆ Windows 2000 或 2000 Server、 XP 或带最新 Service Pack 的 Windows Server 2003 （32 位） ◆ Red Hat Linux 3 或 4 AS 和 ES （32 位和 64 位，虽然 Novell Audit 只运行于 32 位模式） ◆ Solaris 8、 9 或 10 ◆ SUSE Linux Enterprise Server 9 或 10 （32 位和 64 位，虽然 Novell Audit 只运行于 32 位模式） 带最新 Support Pack 和插件的 iManager 2.6 和 2.7。	OES、 NetWare、 Windows 和 Linux 平台（Red Hat 和 SUSE）支持下列所有 32 位模式的处理器： ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 和 Opteron 最低安全服务器要求包括： ◆ 单处理器、服务器级 PC （具有 Pentium* II 400 MHz） ◆ 最少 40 MB 磁盘空间 ◆ 512 MB RAM eDirectory Instrumentation 用于记录 eDirectory 事件，它支持下列 eDirectory 版本： ◆ eDirectory 8.7.3 （NetWare、 Windows、 Linux 和 Solaris） ◆ 带最新 Support Pack 的 eDirectory 8.8 NetWare Instrumentation 允许记录 NetWare 事件，它支持下列 NetWare 版本： ◆ 带最新 Support Pack 的 NetWare 5.1 ◆ 带最新 Support Pack 的 NetWare 6.0 ◆ NetWare 6.5 或带最新 Support Pack 的 NetWare 6.5 ◆ 带最新 Support Pack 的 Novell Open Enterprise Server (OES)

系统组件	系统要求	注释
User Application	应用程序服务器 User Application 运行在 JBoss 和 WebSphere 上，如下所述。 以下各操作系统支持 JBoss 4.2.0： ◆ Novell Open Enterprise Server (OES) 1.0 SP2 或带最新 Support Pack － 仅 Linux ◆ Novell Open Enterprise Server (OES) 2 － SLES 10 SP1 和 NetWare 6.5 SP7 ◆ SUSE Linux Enterprise Server 9 SP2 （包括在 OES 1.0 SP2 中）和 10.1.x （64 位 JVM* ） ◆ 带 SP4 的 Windows 2000 Server （32 位） ◆ 带 SP1 的 Windows 2003 Server （32 位） ◆ Solaris 10 Support Pack （日期为 6/06） 以下各操作系统支持 WebSphere 6.1： ◆ Solaris 10 （64 位模式） ◆ Windows 2003 SP1 以下各操作系统支持 WebLogic 10： ◆ Solaris 10 （64 位模式） ◆ Windows Server 2003 SP1 User Application 需要 JRE* 1.5.0_10 （请参见第 5.1 节 “安装的前提条件。” （第 93 页）） 浏览器 . User Application 同时支持 Firefox 和 Internet Explorer，如下所述。 以下各操作系统支持 Firefox 2： ◆ 带 SP4 的 Windows 2000 Professional ◆ 带 SP2 的 Windows XP ◆ Red Hat Enterprise Linux WS 4.0 ◆ Novell Linux Desktop 9 ◆ SUSE Linux 10.1 ◆ SUSE Linux Enterprise Desktop 10 以下各操作系统支持 Internet Explorer 7： ◆ 带 SP4 的 Windows 2000 Professional ◆ 带 SP2 的 Windows XP ◆ Windows Vista Enterprise V6 以下各操作系统支持 Internet Explorer 6： ◆ 带 SP4 的 Windows 2000 Professional ◆ 带 SP2 的 Windows XP	SUSE Linux Enterprise Server 支持以下 32 位模式下的处理器： ◆ Intel x86 ◆ AMD x86 ◆ Intel EM64T ◆ AMD Athlon64 和 Opteron 采用以下处理器时， SUSE Linux Enterprise Server 将以 64 位模式运行： ◆ Intel EM64T ◆ AMD Athlon64 ◆ AMD Opteron ◆ Sun* SPARC* 在超虚拟化模式下，当 Xen Virtual Machine (VM) 运行 SLES 10 以作为 guest 操作系统时， SUSE Linux Enterprise Server 10 上现在支持 Xen* 虚拟化。需要针对 SLES 10 的 Xen 增补程序 （请参见 TID # 3915180 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3915180&sliceId=SAL_Public&dialogID=20406933&stateId=0%200%2020414606)）。

系统组件	系统要求	注释
User Application 的数据库服务器 ◆ MySQL ◆ Oracle ◆ MS SQL ◆ DB2	JBoss 支持以下数据库： ◆ MySQL V5.0.27 ◆ Oracle 9i （9.2.0.1.0 和 9.2.0.5.0） ◆ Oracle 10g R2 (10.2.0) ◆ MS SQL 2005 SP1 WebSphere 支持以下数据库： ◆ Oracle 10g R2 (10.2.0.) ◆ MS SQL 2005 SP1 ◆ DB2 DV2 v9.1.0.0	User Application 使用数据库来完成各种任务，例如，存储配置数据，以及存储任何正在进行的工作流程活动的数据。 安全日志记录服务以及 User Application 和工作流程供应都需要数据库。可以设置一个数据库同时为两个应用程序提供服务，也可以为每个应用程序设置独立的数据库。安全日志记录服务不包括特定数据库。 瘦客户机驱动程序和 OCI 客户机驱动程序都支持 Oracle。
工作站 ◆ Designer ◆ iManager 万维网访问	已在下列平台上测试了 Designer： Windows： ◆ 带最新 Service Pack 的 Windows 2000 Professional ◆ Windows XP SP2 ◆ 带最新 Service Pack 的 Windows Server 2003 （32 位） ◆ Microsoft Windows Vista Linux： ◆ SUSE Linux Enterprise Server 10 （仅对于 Designer） ◆ SUSE Linux 10.1 ◆ SUSE Linux Enterprise Desktop 10 ◆ Red Hat Linux 4.0 （仅对于 Designer） ◆ Red Hat Fedora* Core 5 （仅对于 Designer） ◆ Novell Linux Desktop 9 ◆ GNOME*、 KDE 和 Red Hat Fedora	Designer 使用 Eclipse 作为其开发平台。有关平台特定信息，请参考 Eclipse 万维网站点 (http://www.eclipse.org/)。 Designer 的最低和建议硬件要求： ◆ 最低 1 GHz，建议 2 GHz 或更高。 ◆ 最低 512 MB RAM，建议 1 GB RAM 或更高。 ◆ 最低 1024 x 768 分辨率，建议 1280 x 1024。 先期必要的软件： ◆ Microsoft Internet Explorer 6.0 SP1 ◆ Microsoft Internet Explorer 7 ◆ 或 Mozilla* Firefox 2.0

系统组件	系统要求	注释
已连接系统服务器（由运行远程装载程序的独立服务器承载） ◆ 远程装载程序 ◆ Remote Loader 配置工具（仅限 Windows） ◆ Novell Audit 代理 ◆ 口令同步代理 ◆ 已连接系统的驱动程序 Shim ◆ 已连接系统的工具	每个驱动程序都要求已连接系统可用，并且提供了相关的 API。 有关每个系统特定的操作系统要求和已连接系统要求，请参考 Identity Manager 驱动程序文档 (http://www.novell.com/documentation/idmdrivers)。	每个连接的应用程序都要求个人具有特定于应用程序的知识并承担相关责任。 Remote Loader System： ◆ Windows NT* 4.0、 Windows 2000 Server 或带最新 Support Pack 的 Windows Server 2003 ◆ 带最新 Service Pack 的 Windows Server 2003 （64 位） ◆ 口令同步代理在 Windows Server 2003 （64 位）上受支持 ◆ Red Hat Linux 3.0、 4.0 和 5.0 ES 及 AS ◆ SUSE Linux Enterprise Server 9 或 10 ◆ Solaris 9 或 10 ◆ AIX 5.2L、 V5.2 和 5.3 Java Remote Loader System： ◆ HP-UX* 11i ◆ OS/400 ◆ zOS* ◆ 应该可以在具有 JVM 1.4.2 或更高版本的任何系统上使用它

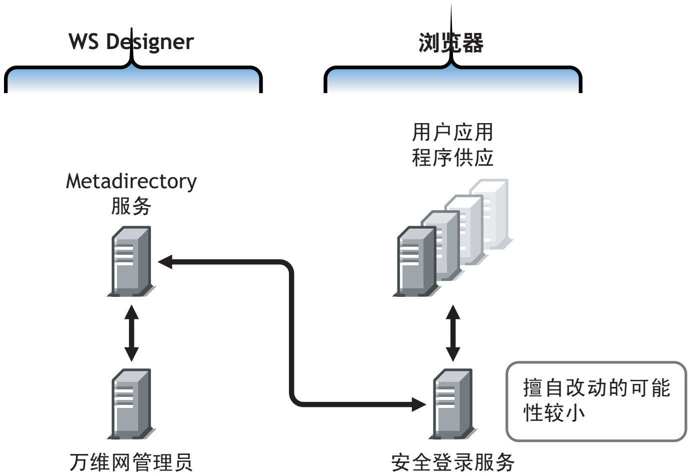
1.6 建议的部署策略

如前所述， Identity Manager 附带有一些必须安装和配置的服务。尽管不建议对生产环境这么做，但可以在一台服务器上安装和配置所有所需服务。或者也可以在每台服务器上部署一项至多项服务。

设计 Identity Manager 部署时，工作负荷是一个主要因素。能够分散的流量越大，应用程序拥有的潜在吞吐量就越大。

图 1-3 展示了一个可用的部署策略，其中 元目录服务使用一台服务器，基于万维网的管理服务使用一台服务器，安全日志记录服务使用一台服务器， User Application 和供应服务使用一台服务器。

图 1-9 Identity Manager 部署策略



元目录服务

部署 Identity Manager 服务的方式取决于服务的工作负荷。例如，可以在一台与已连接系统通讯的服务器上安装 Identity Manager 的元目录服务。只需要在一台运行 eDirectory 的服务器上安装元目录引擎。

由于 iManager 的潜在吞吐量较大，因此您可能不希望将基于万维网的管理服务与元目录服务安装在一起。如果确实要将 iManager 与 Identity Manager 安装在同一台服务器上，请先安装 iManager，然后安装 Identity Manager 及其插件。

基于万维网的管理服务

如果已经在服务器上安装了 iManager 2.6，则只需要运行 Identity Manager 安装，然后安装 iManager 的 Identity Manager 插件。如果要安装 User Application 和供应服务，则还必须运行 User Application 安装，并只安装 iManager 的 User Application 插件。需要针对 User Application 或带有供应模块的 User Application （它们是两个不同的产品）执行此操作。

User Application 和安全日志记录服务

如果执行大量的供应，则建议将 User Application 安装在其自身的服务器上。必要时还可以设置群集。 User Application 包含 MySQL 5.0.27-max，因此，如果将该数据库部署为 User Application 安装的一部分，或者部署为具有供应模块的 User Application 安装的一部分，则不需要设置其他数据库服务。

但是，安全日志记录服务不包括特定的数据库，而安全日志记录服务和 User Application/ 供应服务都需要数据库。可以设置一个数据库为两个应用程序提供服务，也可以为每个服务设置独立的数据库。这取决于执行供应的数量以及日志记录服务的工作负荷。

注释 : 如果要在独立的 （远程）服务器上设置 Oracle 9i 或 10g，则需要安装 Oracle，然后将应用程序服务器配置为提供与数据库的远程连接。

使用 Remote Loader 配置

在安装 Identity Manager 的过程中，如果不需要在已连接系统服务器上安装 eDirectory 服务和元目录引擎，则可以使用*已连接系统*选项。Remote Loader 还通过使用 SSL 技术提供了元

目录引擎和驱动程序之间的安全通讯路径。将系统连接到 Identity Manager 时请记住这一点。

有关规划 Identity Manager 系统的详细信息，请参见第 2 章 “计划”（第 39 页）。

1.7 从何处获取 Identity Manager 及其服务

- 第 1.7.1 节 “安装 Identity Manager 3.5.1”（第 36 页）
- 第 1.7.2 节 “激活 Identity Manager 3.5.1 产品”（第 37 页）

要下载 Identity Manager 及其服务：

1. 转至 Novell 下载万维网站点 (http://download.novell.com)。
2. 在 “产品或技术”菜单中，选择 *Novell Identity Manager*，然后单击 “搜索”。
3. 在 “Novell Identity Manager 下载”页上，单击所需文件旁边的 “下载”按钮。
4. 遵循屏幕提示，将该文件下载到计算机上的某个目录中。
5. 自第 2 步重复操作，直至下载完所有需要的文件。大多数安装需要多个 ISO 映像。

下列 Identity Manager 组件可用于下载。

***表 1-4** ISO 映像的工作方式*

Identity Manager 部件	平台	iso
Identity Manager DVD 用于烧录 DVD 的一个 ISO 映像中提供了下列 Identity Manager 组件。这些组件还可用于每次下载。 ◆ Identity Manager 和驱动程序 ◆ Designer for Identity Manager	Identity Manager： Linux、 NetWare、Windows 和 UNIX* Designer： Linux 和 Windows	Identity_Manager_3_5_1_DVD.iso
Identity Manager 和驱动程序	NetWare 和 Windows	Identity_Manager_3_5_1_NW_Win.iso
Identity Manager 和驱动程序	Linux	Identity_Manager_3_5_1_Linux.iso
Identity Manager 和驱动程序	UNIX	Identity_Manager_3_5_1_Unix.iso
User Application 这是您购买的 Identity Manager 3 中包含的 User Application 的标准版本。	Linux 和 Windows	Identity_Manager_3_5_1_User_Application。iso

Identity Manager 部件	平台	iso
带有 Provisioning Module for Identity Manager 的 User Application 这是 User Application 的 “供应” 版本，它是 Identity Manager 的附加产品，需要单独购买。	Linux 和 Windows	Identity_Manager_3_5_1_User_Application_Provisioning.iso
Designer for Identity Manager	Windows	Identity_Manager_3_5_1_Designer_Win.iso
Designer for Identity Manager	Linux	Identity_Manager_3_5_1_Designer_Linux.iso

购买的 Identity Manager 中包含几个常用客户系统的集成模块，您可能已具有其许可证：Novell eDirectory、Microsoft Active Directory、Microsoft Windows NT、LDAP v3 Directories、Novell GroupWise®、Microsoft Exchange 和 Lotus Notes。其他所有 Identity Manager 集成模块必须单独购买。

User Application 组件位于两个 ISO 映像上：User Application ISO 映像是一个标准版本，包含在购买的 Identity Manage 3 中。带有 Provisioning Module For Identity Manager 的 User Application 是一个附加产品，它集成了功能强大的批准工作流程。该供应模块附带了一个独立的 ISO 映像，需要单独购买该模块。

Identity Manager 采购产品还包含 Designer for Identity Manager，这是一个功能强大且灵活的管理工具，可以显著地简化配置和部署。

1.7.1 安装 Identity Manager 3.5.1

- 要在 Windows、 NetWare、 UNIX 以及 Linux 上安装 Identity Manager 3.5.1，请参见第 4 章 “安装 Identity Manager”（第 63 页）
- 要安装 User Application 或带有供应模块的 User Application，请参见第 5 章 “安装 User Application”（第 93 页）
- 要安装 Designer，请参见 《*Designer 2.1 for Identity Manager 3.5.1* 指南》中的 “ 安装 Designer”。

注释 : Linux 和 UNIX （以前为 NIS）、 Mainframe 和 Midrange 驱动程序安装程序位于 /platform/setup 目录中。这些安装程序必须与 Identity Manager 和 User Application 的安装程序分开运行。

有关已知问题的列表，请参见 Identity Manager 附带的 README 文件。

1.7.2 激活 Identity Manager 3.5.1 产品

Identity Manager 产品需要激活 （Designer 除外）。下列产品可以在 90 天的评估期内使用，之后您必须停止使用这些产品或购买激活。

- Identity Manager 3.5.1
- 带有 Provisioning Module for Identity Manager 的 User Application
- 集成模块

重要：为了成功激活 User Application，必须下载正确的 ISO 映像。例如，如果购买了 Identity Manager，随后又下载了 User Application 供应模块，但没有单独购买供应模块，则 User Application 实施将在 90 天后停止运行。

有关激活的其他信息，请参见第 6 章 “激活 Novell Identity Manager 产品”（第 169 页）。

计划 2

- 第 2.1 节 “计划 Identity Manager 实施的项目管理方面”（第 39 页）
- 第 2.2 节 “常用安装场景的规划”（第 45 页）
- 第 2.3 节 “计划 Identity Manager 实施的技术方面”（第 52 页）

2.1 计划 Identity Manager 实施的项目管理方面

本部分概述了实施 Identity Manager 的高级政策管理和项目管理方面。（有关技术方面的信息，请参见第 2.3 节 “计划 Identity Manager 实施的技术方面”（第 52 页）。）

本规划资料概述了从 Identity Manager 项目的开始到完全生产部署过程中通常要执行的活动的类型。实施身份管理策略过程中，需要发现需求以及环境中的利害关系人、设计解决方案、获得利害关系人的认可以及测试和推行解决方案。本部分旨在帮助您充分了解该过程，以便您能够从 Identity Manager 的使用中获得最大的收益。

强烈建议聘请一个 Identity Manager 专家，便于在解决方案部署的每个阶段随时提供帮助。有关合作伙伴关系选项的更多信息，请参见 Novell® 解决方案合作伙伴万维网站点 (http://www.novell.com/partners/)。 Novell 培训还提供与 Identity Manager 实施有关的课程。

同时还强烈建议设置一个测试 / 开发环境，以便在其中测试、分析和开发解决方案。在情况步入预期轨道后，可将最终产品部署到生产环境中。

本部分并未详尽说明；不旨在讲述所有可能的配置，也不是为了要求严格执行配置。每个环境都存在差异，因此在使用的活动类型上需要灵活处理。

2.1.1 Novell Identity Manager 部署

可以将下列多项活动建议为部署 Identity Manager 时的最佳做法：

- 发现 （第 39 页）
- 需求和设计分析 （第 40 页）
- 概念检验 （第 43 页）
- 数据验证和准备 （第 43 页）
- 试生产 （第 43 页）
- 生产成品计划 （第 44 页）
- 生产部署 （第 44 页）

发现

Identity Manager 实施可以从发现过程开始，该过程实现以下目的：

- 确定身份信息管理的主要目标
- 定义或阐明要解决的业务问题
- 确定解决突出问题需要完成哪些初期工作
- 确定执行其中一项或多项初期工作需要哪些东西

- 制定高级策略或 “解决方案路标”，以及受到认可的执行途径

发现能使所有利害关系人对问题和解决方案达成共识。它为分析阶段提供了一个极好的基础，该阶段需要利害关系人对目录、Novell eDirectory™、Novell Identity Manager 和 XML 集成有一个基本的了解。

- 它可以在所有利害关系人之间建立基本级别的理解
- 它可以从利害关系人那里获得主要业务信息和系统信息
- 它可以促成解决方案路标的制定

发现还将确定紧随其后的步骤，这些步骤可能包括以下项目：

- 确定计划活动，为需求和设计阶段作准备
- 为利害关系人定义其他培训

主要交付内容

- 与主要业务和技术利害关系人进行有序的面谈
- 业务和技术问题的高级摘要报告
- 后续步骤的建议
- 概述发现结果的决策陈述

需求和设计分析

此分析阶段将获得项目的技术和业务方面的细节，并生成数据模型和 Identity Manager 的高级体系结构设计。此活动是至关重要的第一步，解决方案的实施将从这一步开始。

应将设计重心专门放在身份管理上，但是，也可以涉及到通常与资源管理目录 （例如文件和打印）相关的许多要素。下面是可能需要评估的项目的样本：

- 所使用的系统软件的版本是什么？
- 目录设计是否恰当？
- 当前是否使用该目录来承载身份库 和 Identity Manager，或者是否使用它来扩展其他服务？
- 所有系统中的数据质量是否合格？ （如果数据达不到可用的质量，则可能无法根据需要实现业务策略。）
- 环境是否需要数据处理？

完成需求分析后，可为实施建立范围和项目计划，并可确定是否需要执行任何先决活动。为避免出现代价高昂的失误，请尽量完整地收集信息和记录需求。

在需求评估过程中，可能需要完成下列任务：

- 定义业务需求 （第 40 页）
- 分析业务流程 （第 41 页）
- 设计企业数据模型 （第 42 页）

定义业务需求

收集组织的业务过程以及定义这些业务过程的业务需求。

例如，解雇一个员工的业务需求可能是，在解雇该员工的同一天，必须去除该员工的网络和电子邮件帐户访问权限。

下列任务可以引导您定义业务需求：

- 建立流程、过程触发器和数据映射关系。

  例如，如果某事件将在特定过程中发生，那么该过程会导致什么结果？ 将会触发其他哪些过程？
- 在应用程序之间映射数据流。
- 确定从一种格式转换为另一种格式 （例如 2/25/2007 转换为 2007 年 2 月 25 日）需要执行的数据转换。
- 记录存在的数据依赖性。

  如果更改了某个值，则务必要知道该值是否存在依赖性。如果更改了特定的过程，则务必要知道该过程是否存在依赖性。

  例如，选择人力资源系统中某个 “临时”员工状态值，可能意味着 IT 部门需要在 eDirectory 中创建一个用户对象，该用户对象在特定的小时数内对网络的权限和访问权限将受到限制。
- 列出优先级。

  并不是每一方的每个需求、愿望或期望都可以立即实现。设计和部署供应系统的优先级有助于规划路线图。

  将部署划分为多个阶段是很有利的，这样可以先实施部署的某一部分，然后实施部署的其他部分。也可以采取分阶段的部署方法。这种方法应该基于组织中的员工小组。
- 定义前提条件。

  应该记录实施部署的特定阶段所需的先决条件。这包括对需要与 Identity Manager 连接的已连接系统的访问权限。
- 确定授权数据源。

  事先了解系统管理员和经理认为属于他们的信息项目，有助于获取各方的认可并让他们持续认可。

  例如，帐户管理员可能需要为员工授予特定文件和目录访问权限的所有权。在帐户系统中执行本地受托者指派可以达到此目的。

分析业务流程

业务流程的分析通常由会见关键人 （例如实际使用应用程序或系统的经理、管理员和员工）开始。要解决的问题包括：

- 数据源于何处？
- 数据流向何处？
- 数据由何人负责？
- 谁拥有对数据所属业务功能的所有权？
- 需要联系何人更改数据？
- 更改数据牵涉到的各个方面有哪些？
- 数据处理 （收集和 / 或编辑）的工作惯例是什么？
- 执行何种类型的操作？
- 使用什么方法保证数据的质量和完整性？

- 系统驻留在何处 （在哪些服务器上，在哪些部门中）？
- 哪些过程不适用于自动处理？

例如，人力资源的 PeopleSoft 系统管理员可能面临的问题包括：

- 将哪些数据储存在 PeopleSoft 数据库中？
- 员工帐户的各种面板上显示哪些内容？
- 供应系统中需要反映哪些操作 （例如添加、修改或删除）？
- 其中哪些是必需的？ 哪些是可选的？
- 需要根据 PeopleSoft 中执行的操作触发哪些操作 ?
- 要忽略哪些操作 / 事件 / 行为？
- 如何转换数据，以及将其映射到 Identity Manager？

会见关键人可了解组织的其他区域，这样可以更清楚地展现整个过程。

设计企业数据模型

定义业务过程后，可以开始设计反映当前业务流程的数据模型。

模型应该阐明数据的来源、要移至的位置以及不能移至的位置。它还应说明关键事件如何影响数据流。

您还可能希望制作图表，用于演示建议的业务过程以及在该过程中实现自动供应的优势。

此模型的开发由回答类似以下的问题开始：

- 正在移动哪些类型的对象 （用户、组等等）？
- 哪些是相关事件？
- 哪些属性需要同步？
- 在整个业务过程中，针对被管理的各种类型的对象储存了哪些数据？
- 同步是单向还是双向的？
- 哪个系统是哪些属性的权威来源？

考虑系统之间不同值的相互关系也很重要。

例如， PeopleSoft 中的员工状态字段可能有三个设置值：员工、合同工和实习生。但是，Active Directory 系统可能只有两个值：永久和临时。在此情况下，需要确定 PeopleSoft 中的 “合同工”状态，以及 Active Directory 中的 “永久”和 “临时”值。

此工作的重点应是了解每个目录系统、它们如何彼此相关，以及在整个系统中哪些对象和属性需要同步。

主要交付内容

- 数据模型，显示所有系统、授权数据源、事件、信息流和数据格式标准，以及 Identity Manager 中已连接系统和属性之间的映射关系。
- 解决方案的相应 Identity Manager 体系结构
- 附加系统连接要求的详细信息
- 数据验证和记录匹配的策略
- 用于支持 Identity Manager 基础结构的目录设计

相关性

- 熟悉所有外部系统的职员 （如 HR 数据库管理员、网络和讯息系统管理员）
- 系统纲要和样本数据的可用性
- 来自分析和设计阶段的数据模型
- 组织结构图、 WAN 和服务器基础结构等基本信息的可用性

概念检验

此活动的结果是提供一份实验室环境中的实施样本，用于反映公司的业务策略和数据流。该结果基于在需求分析和设计过程中开发的数据模型设计，并且是试生产前的最后一个步骤。

注释 : 此步骤通常有助于获得管理层的支持，以及为最终实施工作获得资金。

主要交付内容

- 在所有系统连接均正常工作的情况下完成的可行的 Identity Manager 概念认证

相关性

- 硬件平台和设备
- 必需软件
- 确定必需连接的分析和设计阶段
- 供测试使用的其他系统的可用性以及对这些系统的访问权限
- 来自分析和设计阶段的数据模型

数据验证和准备

生产系统中数据的质量和一致性可能有所不同，因此同步系统时可能会造成不一致的情况。此阶段明确显示资源实施团队与业务单位或组 （"拥有"或管理系统中要集成的数据）之间的分隔点。相关的风险和成本因素有时可能不属于供应项目。

主要交付内容

- 适合装载进身份库 的生产数据集 （已在分析和设计活动中确定）。这包括可能的装载方法 （批量装载或通过连接程序装载）。同时确定已验证或格式化的数据的要求。
- 同时针对使用的设备以及 Identity Manager 部署的整体分布式结构确定并验证性能因子。

相关性

- 来自分析和设计阶段的数据模型 （建议的记录匹配和数据格式策略）
- 对生产数据集的访问权限

试生产

此活动的目的是开始执行到生产环境的迁移。在此阶段可能有其他自定义操作发生。在此有限的简介中，可确认前面的活动所需的结果，并获得生产成品的协议。

注释：此阶段可提供解决方案的验收准则以及达到全面生产所必需的路标和路线。

主要交付内容

- 试行解决方案，为数据模型以及所需的过程结果提供实时的概念检验和验证

相关性

- 所有以前的活动 （分析和设计、 Identity Manager 技术平台）

生产成品计划

在此阶段中规划生产部署。计划应：

- 确认服务器平台、软件修订版和 Service Pack
- 确认常规环境
- 确认在混合共存中身份库 的简介
- 确认分区和复制策略
- 确认 Identity Manager 实施
- 计划传统过程的交接
- 计划回滚应变策略

主要交付内容

- 生产成品计划
- 传统过程交接计划
- 回滚应变计划

相关性

- 所有以前的活动

生产部署

将在此阶段展开试行解决方案，以影响生产环境中的所有实时数据。它通常遵循这样的协议：试生产符合所有的技术和业务要求。

主要交付内容

- 生产解决方案已准备好进行转换

相关性

- 所有以前的活动

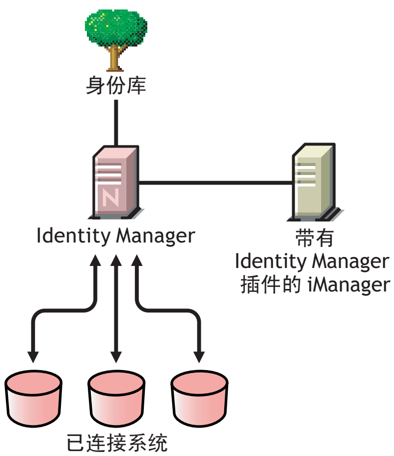
2.2 常用安装场景的规划

以下场景是可能会使用 Identity Manager 的环境的示例。为每个实例提供了一些准则，以帮助您完成实施。

- 第 2.2.1 节 "Identity Manager 的全新安装"（第 45 页）
- 第 2.2.2 节 "在同一环境中使用 Identity Manager 和 DirXML 1.1a"（第 47 页）
- 第 2.2.3 节 "从 Starter Pack 升级为 Identity Manager"（第 49 页）
- 第 2.2.4 节 "从 Password Synchronization 1.0 升级为 Identity Manager 口令同步"（第 50 页）

2.2.1 Identity Manager 的全新安装

图 2-1 *全新安装*



Identity Manager 是一个数据共享解决方案，它可以利用身份库 在应用程序、数据库和目录之间自动同步、转换和分发信息。

Identity Manager 解决方案包括下列组件：

- 带有 Identity Manager 的身份库 （第 45 页）
- 带有 Identity Manager 插件的 iManager Server （第 45 页）
- 已连接系统 （第 46 页）
- 常见的 Identity Manager 任务 （第 46 页）

带有 Identity Manager 的身份库

身份库 包含要与其他已连接系统共享或同步的用户或对象数据。建议将 Identity Manager 安装在其自身的 eDirectory™ 实例中，并将其用作身份库。

带有 Identity Manager 插件的 iManager Server

可以使用 Novell iManager 和 Identity Manager 插件来管理 Identity Manager 解决方案。

已连接系统

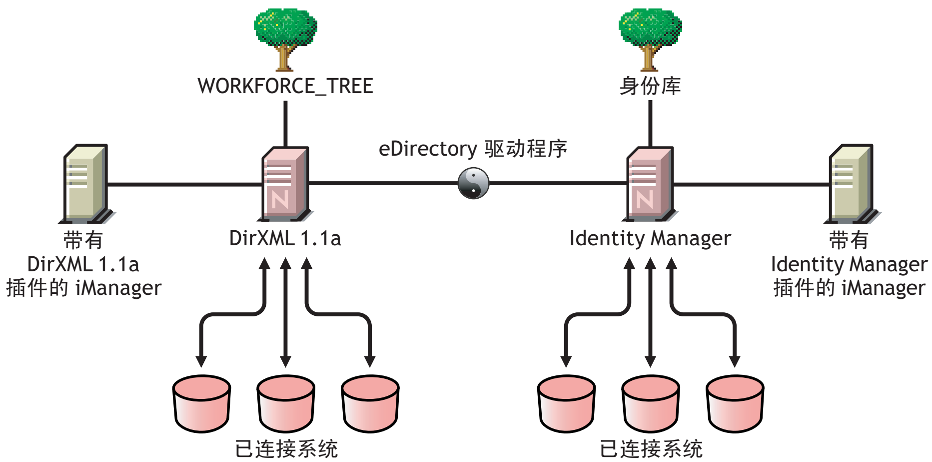
已连接系统可能包含要与身份库 共享或同步数据的其他应用程序、目录和数据库。要在身份库 和已连接系统之间建立连接，请安装该已连接系统的相应驱动程序。有关特定的指导，请参考驱动程序实施指南 (http://www.novell.com/documentation/idm35drivers/index.html)。

常见的 Identity Manager 任务

- **安装系统组件：**由于 Identity Manager 解决方案可能分布在多个计算机、服务器或平台上，因此应该在每个系统上运行安装程序并安装相应的组件。有关更多信息，请参考第 1.4 节 "Identity Manager 安装程序和服务"（第 18 页）。
- **设置已连接系统：**有关特定的指导，请参考第 1.4 节 "Identity Manager 安装程序和服务"（第 18 页）和驱动程序实施指南 (http://www.novell.com/documentation/idm35drivers/index.html)。
- **激活您的解决方案：**Identity Manager 产品 （专业版、服务器版、集成模块和 User Application）需要在安装后的 90 天内激活。请参见第 6 章 "激活 Novell Identity Manager 产品"（第 169 页）。
- **定义业务策略：**通过业务策略，可以自定义特定环境中流入和流出身份库 的信息流。也可利用策略创建新对象、更新属性值、执行纲要转换、定义匹配准则、维护 Identity Manager 关联以及执行其他许多操作。有关策略的详细指南，请参见 《*iManager for Identity Manager 3.5.1 中的策略*》。
- **配置口令管理：**使用口令策略，通过设置用户创建口令的规则，可以提高口令安全性。通过为用户提供用于已忘记口令和重设置口令的自助服务选项，还可以减少帮助中心成本。有关口令管理的详细信息，请参见 "通过使用口令策略管理口令" (http://www.novell.com/documentation/password_management31/index.html?page=/documentation/password_management31/pwm_administration/data/ampxjj0.html)。
- **配置权利：**通过权利定义，可以将已连接系统的权利授予身份库 中定义的用户组。使用权利策略，可以简化业务策略管理，减少配置 Identity Manager 驱动程序的需要。有关更多信息，请参见 《*Novell Identity Manager 3.5.1 管理指南*》中的 "创建和使用权利"。
- **使用 Novell Audit 记录事件：**Identity Manager 配备了 Novell Audit，用于进行审计和报告。Novell Audit 集合了多项技术，提供监视、日志记录、报告和通知功能。通过与 Novell Audit 相集成， Identity Manager 可以提供有关驱动程序和引擎活动当前状态和历史状态的详细信息。这些信息由一组预配置的报告、标准通知服务和用户定义的日志记录提供。请参阅 《*Identity Manager 3.5.1 日志记录和报告*》中的 "使用状态日志"。
- **工作流程批准和 User Application：**Novell Identity Manager User Application 是一个功能强大的万维网应用程序 （和支持工具），用于在复杂的身份服务框架上提供丰富、直观、高度可配置的万维网 UI 体验。当 Identity Manager User Application 与 Provisioning Module for Identity Manager 和 Novell Audit 配合使用时，它可以提供一个完整的、端到端的供应解决方案，具有安全、可伸缩和易于管理的特点。请参见 User Application 文档 (http://www.novell.com/documentation/idm35)。

2.2.2 在同一环境中使用 Identity Manager 和 DirXML 1.1a

图 2-2 在 DirXML 1.1a 所在的同一个树中安装 Identity Manager



如果在同一环境中同时运行 Identity Manager 和 DirXML® 1.1a，请注意下列注意事项：

- 创建身份库 （第 47 页）
- 管理工具 （第 47 页）
- 向后兼容性 （第 47 页）
- 口令管理 （第 48 页）

创建身份库

建议将 Identity Manager 安装在独立的 eDirectory 实例中，并将其用作身份库。

管理工具

- DirXML 1.1a 支持 ConsoleOne®，但 Identity Manager 不支持。
- 需要两个 iManager 服务器，一个用于 DirXML 1.1a 插件，另一个用于 Identity Manager 插件。这是因为插件已得到增强，并且 Identity Manager 使用 DirXML 底稿。
- DirXML 1.1a 的 iManager 插件不能读取在大多数 Identity Manager 驱动程序的已定义驱动程序配置中使用的 DirXML 底稿。
- Designer 是一个使用户能够设计、测试、更新和记录 Identity Manager 驱动程序的工具。

向后兼容性

- 可以在 Identity Manager 服务器上运行 DirXML 1.1a 驱动程序 shim 和配置，并且可以在驱动程序集的 Identity Manager 概述中查看 iManager 中的驱动程序。但是，将驱动程序配置转换为 Identity Manager 格式之前，不能使用 Identity Manager 插件查看或编辑这些驱动程序配置。

  在 Identity Manager 插件中，如果单击某个 1.1a 格式的驱动程序，则系统会提示您完成转换。这是一个通过向导完成的简单过程，并且该过程不会更改驱动程序配置的功能。作为该过程的一部分，将会保存 DirXML 1.1a 版本的备份拷贝。

- 将 DirXML 1.1a 驱动程序与 Identity Manager 引擎一起运行时，这些驱动程序的激活仍然有效。但是，如果将驱动程序 shim 升级为 Identity Manager 版本，则需要获取新的激活身份凭证。有关详细信息，请参见附录 6 “激活 Novell Identity Manager 产品”（第 169 页）。
- 在多数情况下， Identity Manager 驱动程序 shim 可以和 DirXML 1.1a 配置一起运行。有关升级信息，请参见各个驱动程序实施指南 (http://www.novell.com/documentation/idm35drivers/index.html)。

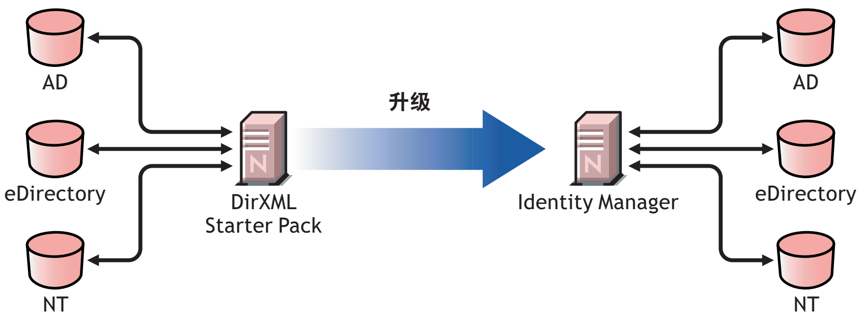
  一个值得注意的例外情况是：在升级驱动程序 shim 后，除非添加某些额外的驱动程序策略，否则 Password Synchronization 1.0 对于 Windows AD 和 Windows NT 不能正常运行。有关指导，请参见 Identity Manager Drivers for Active Directory and NT Domain 的驱动程序实施指南 (http://www.novell.com/documentation/idm35drivers/index.html) 中有关 “口令同步”的部分。
- 不支持将 Identity Manager 驱动程序 Shim 和驱动程序配置与 DirXML 1.1a 引擎一起运行。
- 不支持将 Identity Manager 驱动程序配置与 DirXML 1.1a 驱动程序 Shim 一起运行。
- 如果在多个服务器上运行同一个 Identity Manager 驱动程序配置，请确保这些服务器运行相同的 Identity Manager 版本，并且运行相同的 eDirectory 版本。

口令管理

- 可以创建提供以下功能的口令策略：比如要求使用安全性更高的口令的高级口令规则、为用户提供的忘记口令自助服务和重设置口令自助服务。请参见 Password Management 3.1 Guide (http://www.novell.com/documentation/password_management31/index.html) 中的 “Managing Password Synchronization” 部分。
- 如果开始使用带有 Netware 6.5® 初始发行版的通用口令，则只有在完成某些升级步骤后才能使用新的口令策略功能。请参见 Password Management 3.1 Guide (http://www.novell.com/documentation/password_management31/index.html) 中的 “(NetWare 6.5 only) Deploying Universal Password”。如果开始使用带有 NetWare 6.5 SP2 的通用口令，则不需要该过程。
- Identity Manager 口令同步提供双向口令同步，并且除了支持 Password Synchronization 1.0 以外，还支持其他多种平台。
- 如果您将 Password Synchronization 1.0 与 Windows AD 或 Windows NT 配合使用，在安装新的驱动程序 shim 之前，请确保查看升级指导。请参见第 2.2.4 节 “从 Password Synchronization 1.0 升级为 Identity Manager 口令同步”（第 50 页）。
- 通过提供驱动程序策略 “覆盖”，帮助对现有驱动程序添加双向口令同步功能。请参见《*Novell Identity Manager 3.5.1 管理指南*》中的 “升级现有的驱动程序配置以支持口令同步”。

2.2.3 从 Starter Pack 升级为 Identity Manager

图 2-3 从 Starter Pack 升级为 Identity Manager



其他 Novell 产品中包含的 Identity Manager Starter Pack 解决方案提供了 Nt 域、 Active Directory 和 eDirectory 中所保存信息的许可同步。此外，还包含了其他几个系统 （包括 PeopleSoft、 GroupWise® 和 Lotus Notes）的评估驱动程序，用于查看其他系统的数据同步。

该解决方案还提供了同步用户口令的功能。使用 PasswordSync，用户只需要记住一个口令便可以登录其中任何一个系统。管理员可以管理所选系统中的口令。只要更改了其中一个环境中的某个口令，所有环境中的该口令都会更新。

NetWare 6.5 和 Nterprise™ Linux Services 1.0 附带的 Identity Manager Starter Pack 基于 DirXML 1.1a 技术。从 Starter Pack 升级为 Identity Manager 的最新版本时，请记住下列注意事项：

- 向后兼容性 （第 49 页）
- 口令管理 （第 50 页）
- 激活 （第 50 页）

向后兼容性

- 可以在 Identity Manager 服务器上运行 DirXML 1.1a 驱动程序 shim 和配置，并且可以在驱动程序集的 Identity Manager 概述中查看 iManager 中的驱动程序。但是，将驱动程序配置转换为 Identity Manager 格式之前，不能使用 Identity Manager 插件查看或编辑这些驱动程序配置。

  在 Identity Manager 插件中，如果单击某个 1.1a 格式的驱动程序，则系统会提示您完成转换。这是一个通过向导完成的简单过程，并且该过程不会更改驱动程序配置的功能。作为该过程的一部分，将会保存 DirXML 1.1a 版本的备份拷贝。
- 将 DirXML 1.1a 驱动程序与 Identity Manager 引擎一起运行时，这些驱动程序的激活仍然有效。但是，如果将驱动程序 shim 升级为 Identity Manager 版本，则需要新的激活身份凭证。
- 在多数情况下， Identity Manager 驱动程序 shim 可以和 DirXML 1.1a 配置一起运行。有关升级信息，请参见各个驱动程序实施指南 (http://www.novell.com/documentation/idm35drivers/index.html)。

  一个值得注意的例外情况是：在升级驱动程序 shim 后，除非添加某些额外的驱动程序策略，否则 Password Synchronization 1.0 对于 Windows AD 和 Windows NT 不能正常运行。有关指导，请参见 Identity Manager Drivers for Active Directory and NT Domain 的驱动程序实施指南 (http://www.novell.com/documentation/idm35drivers/index.html) 中有关 “口令同步” 的部分。

- 不支持将 Identity Manager 驱动程序 Shim 和驱动程序配置与 DirXML 1.1a 引擎一起运行。
- 不支持将 Identity Manager 驱动程序配置与 DirXML 1.1a 驱动程序 Shim 一起运行。
- 如果在多个服务器上运行同一个 Identity Manager 驱动程序配置，请确保这些服务器运行相同的 Identity Manager 版本，并且运行相同的 eDirectory 版本。

口令管理

- 升级驱动程序 shim 后，除非添加某些额外的驱动程序策略，否则 Starter Pack (DirXML 1.1a) 所附带的 Password Synchronization 1.0 对于 AD 和 NT 不能正常运行。有关指导，请参见 Identity Manager Drivers for Active Directory and NT Domain 的驱动程序实施指南 (http://www.novell.com/documentation/idm35drivers/index.html) 中有关 "口令同步" 的部分。
- 有关此升级过程的特定指导，请参考第 2.2.4 节 "从 Password Synchronization 1.0 升级为 Identity Manager 口令同步"（第 50 页）。

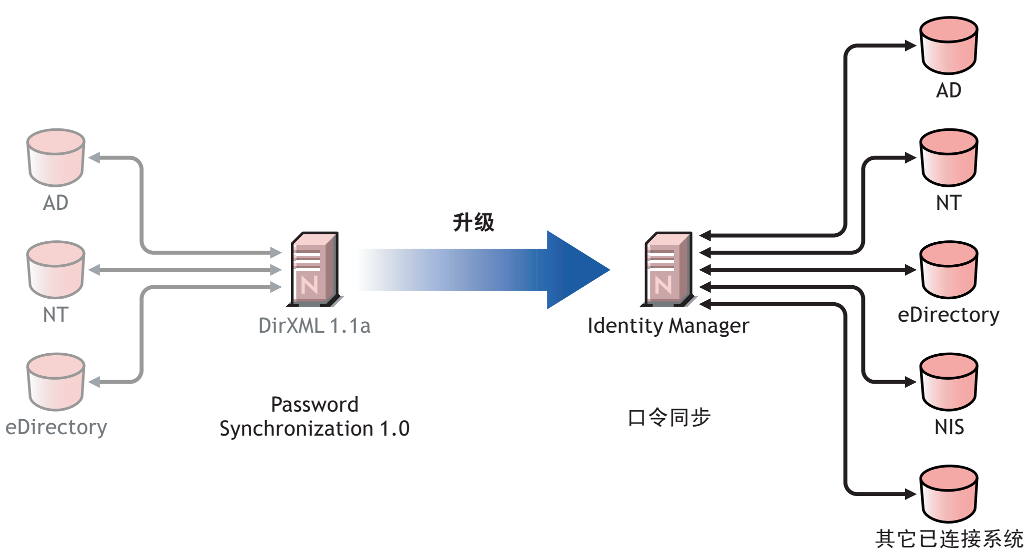
激活

- 所有 Identity Manager 产品都必须在 90 天内激活。如果购买了其他 Novell 软件，DirXML Starter Pack 会包含 DirXML 1.1a 引擎、 NT、 AD 和 eDirectory 驱动程序的激活。从 Identity Manager Starter Pack 升级后，需要重新应用这些驱动程序的激活身份凭证。

  有关激活的更多信息，请参考附录 6 "激活 Novell Identity Manager 产品"（第 169 页）。

2.2.4 从 Password Synchronization 1.0 升级为 Identity Manager 口令同步

图 2-4 从 Password Synchronization 1.0 升级为 Identity Manager 口令同步



Identity Manager 口令同步提供许多功能，包括双向口令同步、附加平台，以及口令同步失败时的电子邮件通知。

如果使用带有 Active Directory 或 NT Domain 的 Password Synchronization 1.0，请务必在安装新的驱动程序 Shim 之前，查看升级指导。

如果运行带有 Password Synchronization 2.0 的 Identity Manager 2.x，则不需要遵循这些步骤。

有关 Identity Manager 口令同步的一般信息，请参见 《*Novell Identity Manager 3.5.1 管理指南*》中的 “在已连接系统间同步口令”。该部分包含概念性信息，包括新旧功能的比较、先决条件、每个已连接系统支持的功能的列表、向现有驱动程序添加支持的指导以及显示新功能使用方式的多个场景。

本部分包括：

- 对 Active Directory 或 Windows NT 升级口令同步 （第 51 页）
- 升级 eDirectory 的口令同步 （第 51 页）
- 升级其他已连接系统驱动程序 （第 52 页）
- 处理敏感信息 （第 52 页）

对 Active Directory 或 Windows NT 升级口令同步

新的口令同步功能是由驱动程序策略执行的，而不是由独立的代理执行的。这意味着，如果安装新驱动程序 shim 的同时不升级驱动程序配置，则 Password Synchronization 1.0 只对现有用户仍然有效。在完成驱动程序配置的升级之前，新用户、已移动的用户或重命名的用户不参与口令同步。

使用下列常规步骤进行升级：

1. 升级环境使之支持通用口令，包括升级 Novell Client™ （如果使用的话）。
2. 安装 Identity Manager 3.5.1 驱动程序 shim，以替换 Active Directory 或 Windows NT 的 DirXML 1.1a 驱动程序 shim。
3. 将新的策略添加到驱动程序配置，立即创建 Password Synchronization 1.0 的向后兼容性。

   执行该步骤后，在切换到 Identity Manager 口令同步之前， Password Synchronization 1.0 可持续正常运行。
4. 通过驱动程序策略添加对新 Identity Manager Password Synchronization 的支持。
5. 安装和配置新的口令同步过滤器。
6. 必要时设置 SSL。
7. 必要时通过使用口令策略打开通用口令。
8. 设置需要使用的 Identity Manager Password Synchronization 场景。

   请参见 《*Novell Identity Manager 3.5.1 管理指南*》中的 “实施口令同步”。
9. 去除 Password Synchronization 1.0

有关详细指导，请参见 Identity Manager Drivers for Active Directory and NT Domain 的驱动程序实施指南 (http://www.novell.com/documentation/idm35drivers/index.html)。

升级 eDirectory 的口令同步

升级 eDirectory 相当简单，并且，如果驱动程序 shim 和配置具有最新增补程序，则驱动程序 shim 将和现有 DirXML 1.1a 驱动程序配置一起运行且不发生更改。有关指导，请参见《*Identity Manager 3.5.1 Driver for eDirectory：实施指南*》。

升级其他已连接系统驱动程序

除了支持 Password Synchronization 1.0 以外， Identity Manager 口令同步还支持其他许多已连接系统。

有关受支持的其他系统的功能列表，请参见 《*Novell Identity Manager 3.5.1 管理指南*》中的 " 口令同步支持的已连接系统 "。

通过提供驱动程序策略 "覆盖"，帮助对以前不支持的已连接系统的现有驱动程序添加双向口令同步功能。请参见 《*Novell Identity Manager 3.5.1 管理指南*》中的 "升级现有的驱动程序配置以支持口令同步"。

处理敏感信息

通用口令受 eDirectory 中四个加密层保护，因此在该环境中是非常安全的。如果选择使用双向口令同步，并且使通用口令与分发口令同步，请注意这是在提取 eDirectory 口令并将它发送到其他已连接系统。需要对口令的传输加以保护，同时还要保护同步口令的已连接系统。

在同步口令的同时，还可以使用 Novell SecretStore® 和 Novell SecureLogin 来同步身份凭证。在需要认可的环境中，通过它们可以提供 SecureLogin 通行口令问题和答案。请参见 《*Novell Identity Manager 3.5.1 管理指南*》中的 "安全：最佳实践"。

2.3 计划 Identity Manager 实施的技术方面

- 第 2.3.1 节 "使用 Designer"（第 52 页）
- 第 2.3.2 节 "在服务器上复制 Identity Manager 需要的对象"（第 52 页）
- 第 2.3.3 节 "使用 "范围过滤" 管理不同服务器上的用户"（第 53 页）

2.3.1 使用 Designer

Identity Manager 附带一个名为 Designer 的实用程序。 Designer 可用于设计、测试和记录 Identity Manager 驱动程序。Designer 还可用于查看口令同步和数据流动的方式。有关更多信息，请参见 《*Designer 2.1 for Identity Manager 3.5.1 管理指南*》。

2.3.2 在服务器上复制 Identity Manager 需要的对象

如果 Identity Manager 环境访问多个服务器以运行多个 Identity Manager 驱动程序，那么规划时要确保在运行这些 Identity Manager 驱动程序的服务器上复制某些 eDirectory 对象。

只要已过滤复本中包括驱动程序需要读取或同步的所有对象和属性，就可以使用这些复本。

请记住，必须为 Identity Manager 驱动程序对象授予对任何要同步的对象的足够 eDirectory 权限，方法是通过显式授权，或者使驱动程序对象的安全性等效于具有所需权限的对象。

运行 Identity Manager 驱动程序的 eDirectory 服务器 （如果使用远程装载程序，则是驱动程序参照的 eDirectory 服务器）必须保存下列主复本或读 - 写复本：

- 该服务器的驱动程序集对象。

  运行 Identity Manager 的每个服务器都应该具有一个驱动程序集对象。除非有特定的需求，否则不要将多个服务器与同一个驱动程序集对象关联。

注释：当创建驱动程序集对象时，默认设置是创建独立的分区。Novell 建议在驱动程序集对象上创建独立的分区。要使 Identity Manager 正常运行，服务器需要保存驱动程序集对象的完整复本。如果服务器具有驱动程序集对象的安装位置的完整复本，则不需要分区。

- 该服务器的服务器对象。

  服务器对象是必需的，因为驱动程序使用它为对象生成密钥对。对于 Remote Loader 鉴定来说，它也至关重要。

- 需要同步驱动程序的该实例的对象。

  除非这些对象的复本与驱动程序位于同一台服务器上，否则驱动程序不能同步对象。事实上， Identity Manager 驱动程序将同步在服务器上复制的*所有*树枝中的对象，除非您创建规则以另行指定 （用于范围过滤的规则）。

  例如，如果需要驱动程序同步所有用户对象，最简单的方法是使用驱动程序的一个实例，该驱动程序位于保存所有用户的主复本或读 / 写复本的服务器上。

  但是，许多环境都没有包含所有用户复本的单台服务器。相反，完整用户集分布在多台服务器上。在这种情况下，有三种选择：

  - **将用户聚合到单台服务器。**可通过向现有服务器添加复本来创建保存所有用户的单台服务器。如果需要，只要必需的用户对象和属性是已过滤复本的一部分，就可以使用已过滤复本减少 eDirectory 数据库的大小。
  - **在启用范围过滤的情况下，使用多台服务器上的驱动程序的多个实例。**如果不希望将用户聚合到单台服务器，则需要确定由哪个服务器集保存所有用户，同时在其中的每个服务器上设置 Identity Manager 驱动程序的一个实例。

    为防止驱动程序的不同实例尝试同步相同的用户，您将需要使用范围过滤来定义每个驱动程序实例应该同步的用户。范围过滤表示向每个驱动程序添加规则，以将驱动程序的管理范围限制到特定的树枝。请参见使用 "范围过滤" 管理不同服务器上的用户 （第 53 页）。
  - **在没有范围过滤的情况下，使用多台服务器上的驱动程序的多个实例。**如果要在不同服务器上运行驱动程序的多个实例且不使用已过滤复本，则需要对不同的驱动程序实例定义策略，以使驱动程序能够处理同一身份库 中的不同对象集。

- 创建用户时需要驱动程序使用的模板对象 （如果选择使用模板）。

  Identity Manager 驱动程序不要求指定用于创建用户的 eDirectory 模板对象。但是，如果指定在 eDirectory 中创建用户时驱动程序应使用模板，则必须在运行驱动程序的服务器上复制模板对象。

- Identity Manager 驱动程序管理用户时需要使用的任何树枝。

  例如，如果创建了一个名称为 "非活动用户" 的树枝以保存禁用的用户帐户，则必须使运行驱动程序的服务器上具有该树枝的主复本或读 / 写复本 （最好是主复本）。

- 驱动程序需要参照的其他任何对象 （例如， Avaya* PBX 驱动程序的工作指令对象）。

  如果驱动程序只是读取而不是更改其他对象，则服务器上的这些对象的复本可以是只读复本。

2.3.3 使用 "范围过滤" 管理不同服务器上的用户

"范围过滤" 表示向每个驱动程序添加规则，以将驱动程序的操作范围限制到特定的树枝。在以下两种情况下，可能需要使用范围过滤：

- 希望驱动程序只同步特定树枝中的用户。

默认情况下， Identity Manager 驱动程序将同步运行该驱动程序的服务器上复制的所有树枝中的对象。要缩小该范围，必须创建范围过滤规则。

- 希望 Identity Manager 驱动程序同步所有用户，但不希望在同一服务器上复制所有用户。

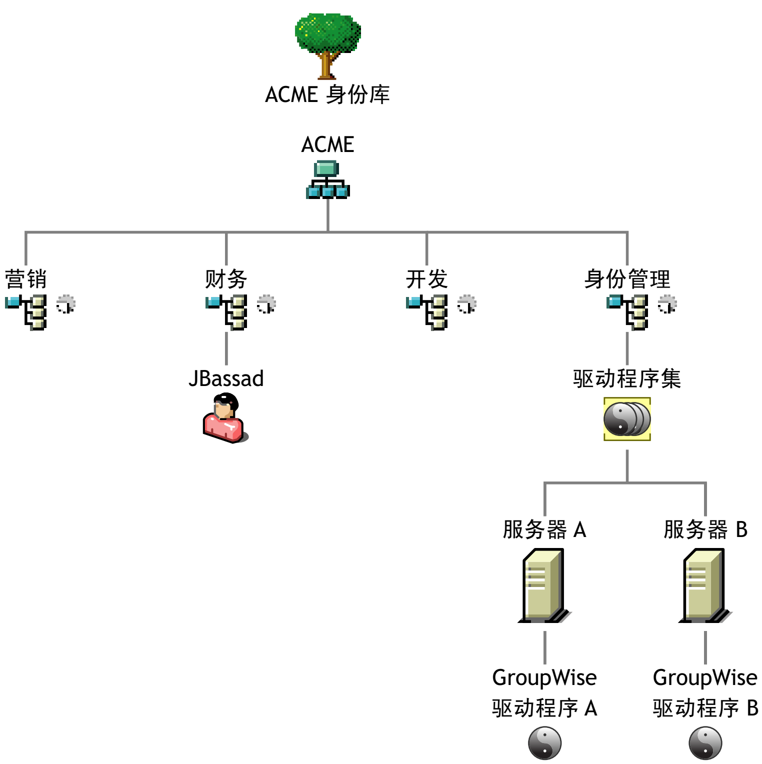
  要同步所有用户且不将其复制到单台服务器上，则需要确定由哪个服务器集保存所有用户，然后在其中的每台服务器上创建 Identity Manager 驱动程序的实例。为防止驱动程序的两个实例尝试与相同的用户同步，您将需要使用 “范围过滤”来定义驱动程序的每个实例应该同步的用户。

注释 : 即使服务器的复本当前未重叠，也应该使用范围过滤。以后，服务器上可能会添加复本，因而可能无意中产生重叠。如果实施了范围过滤， Identity Manager 驱动程序就不会尝试同步相同的用户，即使以后向服务器添加复本，也是如此。

下面给出了如何使用范围过滤的示例：

下图显示了一个身份库，它带有三个保存用户的树枝：市场营销、财务和开发。同时它还显示了保存驱动程序集的 Identity Manager 树枝。其中每个树枝都是一个独立的分区。

图 2-5 范围过滤的示例树



在此示例中， Identity manager 管理员有两个身份库 服务器：服务器 A 和服务器 B，如图 2-6 （第 55 页）所示。两个服务器都不包含所有用户的拷贝。每个服务器包含三个分区中的两个，因此服务器保存项目的范围重叠。

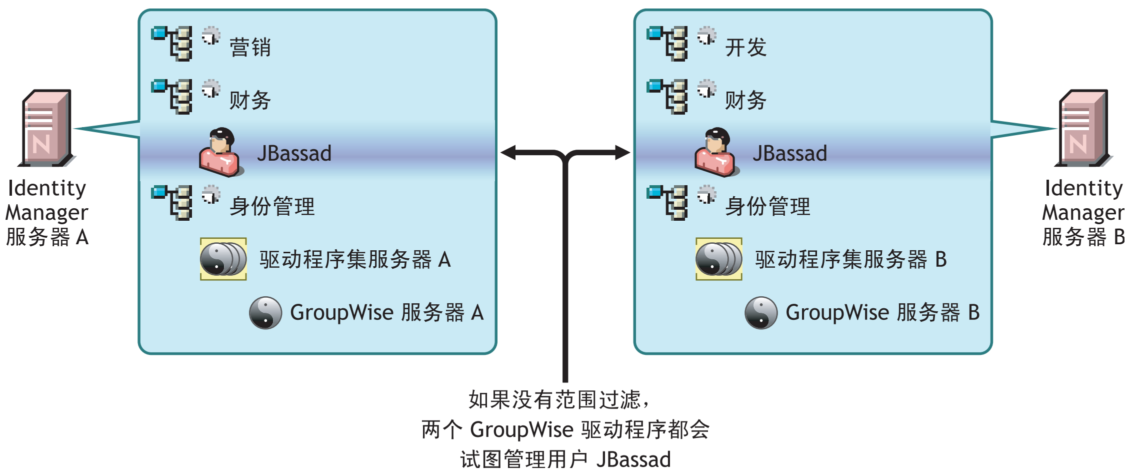
管理员希望通过 GroupWise 驱动程序同步树中的所有用户，但是不希望将这些用户的复本聚合到单台服务器。他选择使用 GroupWise 驱动程序的两个实例，每台服务器使用一个。他在每台 Identity Manager 服务器上安装 Identity Manager，然后设置 GroupWise 驱动程序。

服务器 A 保存 “市场营销” 和 “财务” 树枝的复本。同时， Identity Management 树枝的复本也在该服务器上，该树枝保存服务器 A 的驱动程序集以及服务器 A 的 GroupWise 驱动程序对象。

服务器 B 保存 Development 和 Finance 树枝的复本，同时， Identity Management 树枝也在该服务器上，该树枝保存服务器 B 的驱动程序集和服务器 B 的 GroupWise 驱动程序对象。

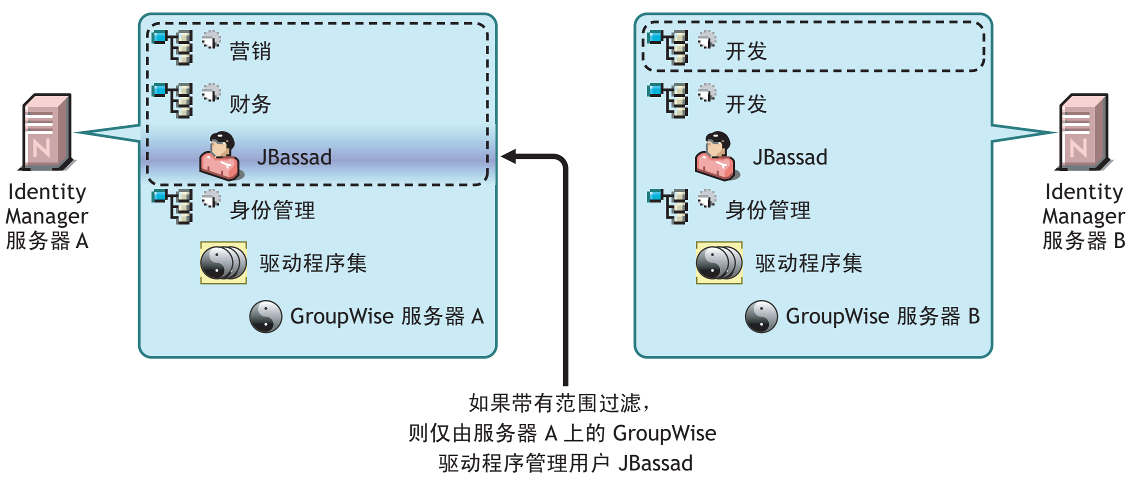
由于服务器 A 和服务器 B 均保存了 “财务” 树枝的复本，因此这两个服务器均保存了 “财务” 树枝中的用户 JBassad。如果不使用范围过滤， GroupWise 驱动程序 A 和 GroupWise 驱动程序 B 都会同步 Jbassad。

图 2-6 带重叠复本的两个服务器，不使用范围过滤



下图显示由于范围过滤已定义了由哪些驱动程序同步每个树枝，因此它可以防止驱动程序的两个实例管理相同的用户。

图 2-7 范围过滤定义由哪些驱动程序同步每个树枝



Identity Manager 3.5.1 附带了一些预定义的规则。有两个规则可帮助执行范围过滤。“事件转换 — 范围过滤 — 包含子树” 和 “事件转换 — 范围过滤 — 不包括子树” 在 *了解 Identity Manager 的策略*中有所论述。

对于此示例，可以对服务器 A 和服务器 B 使用 “包括子树”预定义规则。可为每个驱动程序定义不同的范围，以便它们只同步指定树枝中的用户。服务器 A 将同步 “市场营销”和 “财务”。服务器 B 将同步 “开发”。

升级 3

Identity Manager 有许多不同的组成部分。要升级 Identity Manager，需要确保已考虑了产品的各个方面，这样升级才能成功。

- 第 3.1 节 “升级路径”（第 57 页）
- 第 3.2 节 “策略体系结构的更改”（第 57 页）
- 第 3.3 节 “升级过程”（第 58 页）
- 第 3.4 节 “升级口令同步”（第 60 页）
- 第 3.5 节 “从 RNS 升级到 Novell Audit”（第 61 页）
- 第 3.6 节 “升级 DirXML 1.1a 驱动程序配置”（第 61 页）
- 第 3.7 节 “激活 Identity Manager”（第 61 页）

中说明了一些升级方案。第 2.2 节 “常用安装场景的规划”（第 45 页）

3.1 升级路径

下表包含 Identity Manager 各版本所支持的升级方案。以支持或不支持的形式列出了每种方案。

***表 3-1** 升级路径方案*

安装的版本	当前版本	是否支持升级?
DirXML® 1.1a	Identity Manager 3.5.1	是
Identity Manager 2.x	Identity Manager 3.5.1	是
Identity Manager 3.0.x	Identity Manager 3.5.1	是

3.2 策略体系结构的更改

Identity Manager 3.5 和 3.5.1 包含更新的策略体系结构，该体系结构影响驱动程序参照策略的方式。由于 3.5.1 驱动程序体系结构在 3.5.1 环境中提供了更多的功能，因此 3.0.x 元目录引擎无法运行 3.5.1 驱动程序配置。

但是， Identity Manager 3.5 和 3.5.1 能运行 3.0x 驱动程序配置。如果您的 3.0.x 驱动程序配置同时与 3.0.x 和 3.5.1 元目录引擎关联，则不要升级 3.0.x 驱动程序。虽然 3.0.x 驱动程序配置在 3.5.1 环境中工作，但是它们不具有 Identity Manager 3.5 及更高版本提供的更多功能。当 3.0.x 驱动程序配置只与 3.5 或更新的元目录引擎关联时，您应该将 3.0.x 驱动程序升级到 3.5.1。

有关策略体系结构以及将驱动程序升级到 3.5.1 的更多信息，请参见《*了解 Identity Manager 3.5.1 的策略*》中的 “升级 Identity Manager 策略”。

3.3 升级过程

要成功地升级到 Identity Manager 3.5.1，需要完成下列步骤。

- 第 3.3.1 节 “导出驱动程序”（第 58 页）
- 第 3.3.2 节 “校验最低要求”（第 59 页）
- 第 3.3.3 节 “升级引擎”（第 59 页）
- 第 3.3.4 节 “升级 Remote Loader”（第 60 页）
- 第 3.3.5 节 “UNIX/Linux 环境中的升级”（第 60 页）

3.3.1 导出驱动程序

升级之前，最重要的步骤是备份当前驱动程序及其配置信息。要备份驱动程序，需要将其导出。

- 从 ConsoleOne 导出 （第 58 页）
- 从 iManager 导出 （第 58 页）
- 从 Designer 导出 （第 59 页）

从 ConsoleOne 导出

1. 在 Consoleone® 中，右键点击驱动程序集对象，然后选择*属性 > DirXML > 驱动程序*。
2. 选择要为其创建导出的驱动程序，然后单击*导出*。
3. 指定文件名。保留默认的扩展名 .Xml，然后单击*保存*。
4. 单击*导出配置*。

在 iManager 中，可以导出一个驱动程序，也可以导出整个驱动程序集。如果导出驱动程序集，则会创建单个配置文件。如果导出每个驱动程序，则为每个驱动程序创建一个配置文件。

从 iManager 导出

1. 在 iManager 中选择 *Dirxml 实用程序 > 导出驱动程序*。
2. 浏览并选择要导出的驱动程序或驱动程序集，然后单击 *下一步*。
3. 将提示字段留空，以便按原样创建驱动程序的拷贝，然后单击 *下一步*。
4. 如果选择 “驱动程序集”对象，则对于每个驱动程序均会收到相应提示页。将每个驱动程序的字段留空，以便按原样创建拷贝。
5. 单击 “另存为”。
6. 在 “文件下载”窗口单击 “保存”。
7. 浏览并指定文件位置和导入的名称，然后单击 “保存”。

重要 : 保存文件时，需要使用文件扩展名 .xml。

完成驱动程序的导出后，可在实验室环境下测试导出的驱动程序。导入驱动程序导出并测试驱动程序，以确保所有参数正确，且没有丢失任何功能。

从 Designer 导出

1 在 Designer 的 “模型程序” 视图中右键单击驱动程序或驱动程序集对象，然后单击*导出为配置文件*。

2 在 “导出驱动程序配置” 窗口中，浏览并指定导出的文件位置和名称，然后单击*保存*。

3.3.2 校验最低要求

要升级到 Identity Manager 3.5.1，运行 Identity Manager 服务的服务器需满足最低要求。有关每个平台的最低要求的列表，请参见表 1-3 （第 28 页）。

如果需要升级支持组件，请按以下顺序完成升级：

1. 将操作系统升级为受支持的版本。例如，将 NetWare® 6.0 升级到 NetWare 6.5。
2. 将 eDirectory™ 升级到带最新 Support Pack 的 eDirectory 8.7.3.6，或升级到带最新 Support Pack 的 eDirectory 8.8。
3. 必须具有带 NMAS™ 3.1.3 的 Security Services 2.0.5，以支持 SSL。
4. 将 iManager 升级到带最新 Support Pack 的 iManager 2.6 或 2.7 （包括升级到 Apache 2.0.52 或更新版本和 Tomcat 4.1.18 或更新版本）
5. 还必须在网络上安装 Novell® Audit 2.0.2 Starter Pack 或 Sentinel™ 5.1.3。
6. 有关 Identity Manager User Application 和供应，请参见第 5.1 节 “安装的前提条件。” （第 93 页）。
7. 升级 Identity Manager。
8. 激活 元目录引擎和任何已升级的驱动程序。

3.3.3 升级引擎

升级支持组件后，即会升级 DirXML 或 Identity Manager 引擎。

1 升级前，请确保已导出驱动程序并且有效。请参见第 3.3.1 节 “导出驱动程序”（第 58 页）。

2 停止驱动程序。

  2a 在 iManager 中，选择 *Identity Manager > Identity Manager 概述*。

  2b 浏览并选择驱动程序集对象，然后单击*搜索*。

  2c 单击驱动程序图标的右上角，然后选择*停止驱动程序*。

3 将驱动程序设置为手动启动。

  3a 在 iManager 中，选择 *Identity Manager > Identity Manager 概述*。

  3b 浏览并选择驱动程序集对象，然后单击*搜索*。

  3c 在驱动程序图标右上角，单击*编辑属性*。

  3d 在 “驱动程序配置” 页中的*启动选项*下选择*手动*。

4 安装 Identity Manager 3.5.1。

  升级到 Identity Manager 3.5.1 的步骤与安装 Identity Manager 3.5 的步骤相同。有关如何安装 Identity Manager 的指导，请参见第 4 章 “安装 Identity Manager”（第 63 页）。

  Identity Manager 3.5.1 复制了 Identity Manager 的先前版本，更新了二进制数据。iManager 和 Designer 均更新驱动程序以获取新的功能。

4a 在 iManager 中，单击驱动程序可启动驱动程序升级向导。

当 Designer 检测到旧的驱动程序时，它会自动启动驱动程序升级向导。

5 设置驱动程序启动选项。

5a 在 iManager 中，选择 *Identity Manager* > *Identity Manager 概述*。

5b 浏览并选择驱动程序集对象，然后单击*搜索*。

5c 在驱动程序图标右上角，单击*编辑属性*。

5d 在 "驱动程序配置" 页中的*启动选项*下，选择*自动启动*，或选择启动驱动程序的首选方法。

6 查看驱动程序参数和策略，确保一切均按需要进行设置。

7 启动驱动程序。

7a 在 iManager 中，选择 *Identity Manager* > *Identity Manager 概述*。

7b 浏览并选择驱动程序集对象，然后单击*搜索*。

7c 单击驱动程序图标的右上角，然后选择*启动驱动程序*。

3.3.4 升级 Remote Loader

如果运行 Remote Loader，则还需要升级 Remote Loader 文件。

1. 创建 Remote Loader 配置文件的备份。文件的默认位置如下：
   - Windows C:\Novell\RemoteLoader\ *remoteloadername*-config.txt
   - Linux：在 rdxml 路径中创建自己的配置文件。
2. 停止 Remote Loader 服务或守护程序。
3. 运行 Remote Loader 的安装程序。

   这将文件和二进制数据更新为最新版本。请参见 《*Novell Identity Manager 3.5.1 管理指南*》中的 "安装 Remote Loader"。

3.3.5 UNIX/Linux 环境中的升级

在 UNIX 或 Linux 环境下将 Identity Manager 3.0.1 升级到 Identity Manager 3.5.1 时，将创建两个卸装位置，且不完全去除包。例如，如果在 UNIX 平台 （如 SLES 9）上安装 Identity Manager 3.0.1，则 Identity Manager 卸装程序将位于 /root/dirXML 目录。通过键入 rpm -qa | grep -i dxml，可以显示 dxml 包的安装日期。

如果现在将该部署升级到 Identity Manager 3.5.1，由于命名发生变化，将会在 /root/idm 目录中创建一个新的卸装位置。通过键入 rpm -qa，可以显示更新包的安装日期。

由于目录发生改变，如果管理员卸装 Identity Manager 3.5.1，即使提示已成功去除所有项目，卸装程序也不会去除所有包。要删除剩余的程序包，请使用 DirXML 卸装程序。

3.4 升级口令同步

如果从 DirXML 1.1a 升级到 Identity Manager 3.5.1，则需要对口令同步进行升级。请参见《*Novell Identity Manager 3.5.1 管理指南*》中的 "升级 Password Synchronization 1.0"。

如果从 Identity Manager 2.x 升级，则不执行升级，原因是口令同步相同。

3.5 从 RNS 升级到 Novell Audit

如果当前正在使用 “报告和通知服务” (RNS)，虽然引擎可继续处理 RNS 功能，但还是建议停止使用 RNS。由于 Novell Audit 扩充了 RNS 的功能，并且 Identity Manager 将来的发行版可能将不支持 RNS，因此建议使用 Novell Audit。

有关更多信息，请参见 *Identity Manager 3.5.1 日志记录和报告*中的 “查询和报告”。

3.6 升级 DirXML 1.1a 驱动程序配置

如果从 DirXML 1.1a 升级到 Identity Manager 3.5.1，则将升级驱动程序配置。升级驱动程序配置有两个方面的问题：

- 将 DirXML 规则转换为 Identity Manager 策略。该操作可通过转换工具完成，同时不会增强驱动程序的功能。不需要此转换即可运行旧的驱动程序，但可以通过转换查看 Identity Manager iManager 插件中的现有驱动程序配置。

  需要进行充分的测试，以确保此步骤正常运行。同时还强烈建议设置一个测试 / 开发环境，以便在其中进行解决方案的测试、分析和开发。在情况步入预期轨道后，可将最终产品部署到生产环境中。
- 升级驱动程序策略以添加新功能。例如，对于 Identity Manager 以前使用样式表实现的功能，现在改为使用 DirXML 底稿实现。此级别的功能最好请 Identity Manager 专家进行处理。

请参见 《*Novell Identity Manager 3.5.1 管理指南*》中的 “将驱动程序配置由 DirXML 1.1a 升级为 Identity Manager 3.5.1 格式” 和 “在 Identity Manager 环境中管理 DirXML 1.1a 驱动程序”。

另一种做法是首先进行 Identity Manager 驱动程序配置，然后自定义这些配置，使它们的功能与 DirXML 1.1a 配置的功能相同。

3.7 激活 Identity Manager

升级完成后，需要在 90 天内激活元目录引擎和任何已升级的驱动程序。如果不激活引擎和驱动程序，它们将在 90 天后停止工作。有关激活 Identity Manager 的指导，请参见第 6 章 “激活 Novell Identity Manager 产品”（第 169 页）。

安装 Identity Manager

4

本部分包含安装 Identity Manager 和 Identity Manager 驱动程序的要求和指导。

- 第 4.1 节 “安装前”（第 63 页）
- 第 4.2 节 “Identity Manager 组件和系统要求”（第 63 页）
- 第 4.3 节 “在 NetWare 上安装 Identity Manager”（第 63 页）
- 第 4.4 节 “在 Windows 上安装 Identity Manager”（第 69 页）
- 第 4.5 节 “在 Windows 上安装已连接系统选项”（第 75 页）
- 第 4.6 节 “在 UNIX/Linux 平台上通过 GUI 界面安装 Identity Manager”（第 79 页）
- 第 4.7 节 “在 UNIX/Linux 平台上使用控制台安装 Identity Manager”（第 83 页）
- 第 4.8 节 “在 UNIX/Linux 上使用控制台安装已连接系统选项”（第 86 页）
- 第 4.9 节 “Identity Manager 的非根安装”（第 88 页）
- 第 4.10 节 “安装后的任务”（第 91 页）
- 第 4.11 节 “安装自定义驱动程序”（第 91 页）

4.1 安装前

安装 Identity Manager 之前，请参考第 2 章 “计划”（第 39 页）。

4.2 Identity Manager 组件和系统要求

Novell® Identity Manager 包括可安装在多系统和多平台环境下的组件。根据系统配置的不同，可能需要多次运行 Identity Manager 安装程序才能在相应的系统上安装 Identity Manager 组件。

表 1-3 “Identity Manager 系统组件和系统要求”（第 28 页）列出了 Identity Manager 的安装组件以及对每种系统的要求。

4.3 在 NetWare 上安装 Identity Manager

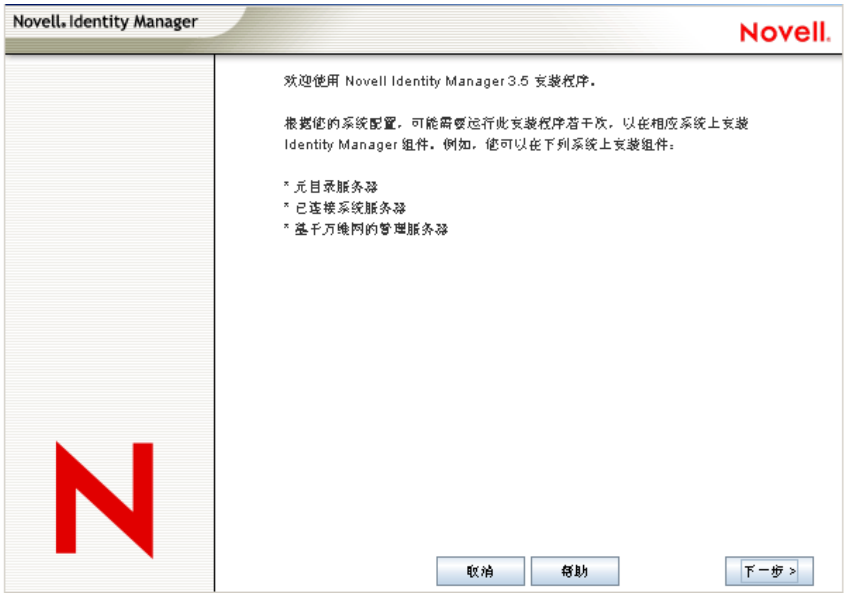
该过程包括适用于 Netware® 的元目录服务器、万维网组件和实用程序的安装。开始之前，请确保系统符合第 4.2 节 “Identity Manager 组件和系统要求”（第 63 页）中列出的要求。

1. 下载所需的 Identity Manager .iso 映像文件。可以从 Novell 下载站点 (http://download.novell.com) 下载 Identity Manager .iso 映像文件。

   Identity Manager 的 NetWare 安装位于 Identity_Manager_3_5_1_NW_Win.iso 或 Identity_Manager_3_5_1_DVD.iso 上。
2. 解压文件并将映像文件存到磁盘上之后，将磁盘插入服务器的 CD 驱动器中，使磁盘作为一个卷装入。
3. 起动 NetWare GUI （在服务器控制台提示符下输入 STARTX），然后选择 *Novell > 安装*。

4 在 “安装的产品”窗口，选择*添加*，然后指定 \NW 目录中 Identity Manager product.ini 文件的路径。单击*确定*，然后再次单击*确定*开始装载 Identity Manager 安装程序。

5 完成文件的复制后，将显示 “Identity Manager 产品安装”页。单击 *下一步*开始安装。



6 选择查看许可证协议的语言，或者使用默认语言 （英语）。

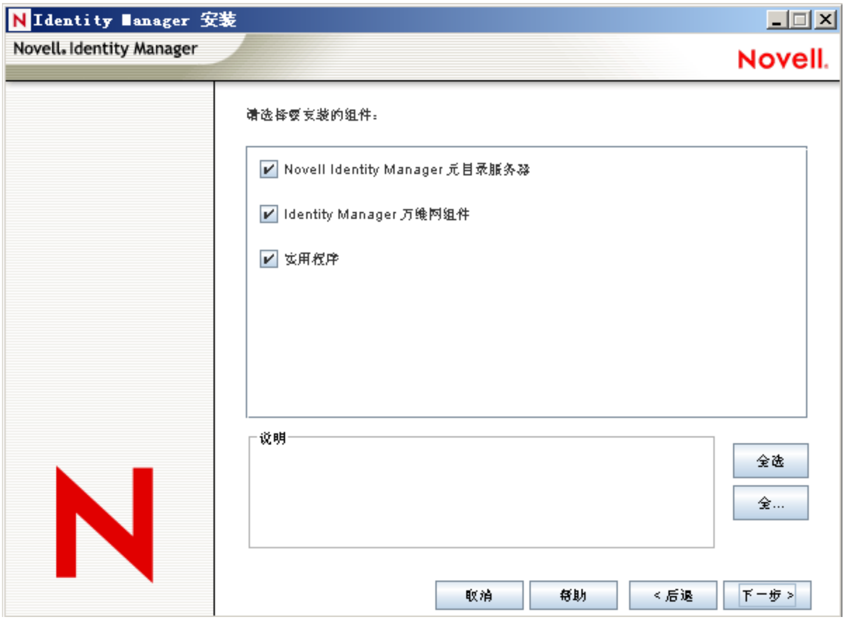
Identity Manager 安装程序将自动以安装程序的计算机上所使用的语言运行。如果安装程序没有被翻译为该计算机所使用的语言，则默认使用英语。

7 阅读许可证协议，然后单击*我接受*。

8 查看说明系统类型 （包括 “元目录服务器”、“万维网组件”和 “实用程序”）的 “概述”页，然后单击 *下一步*继续。

表 1-3 （第 28 页）也对此信息进行了说明。

9 在 “Identity Manager 安装”页上，选择要安装的组件。请参见表 1-3 （第 28 页）。



可用选项如下。大多数安装情况下，可以选择所有的组件。

- **元目录服务器：**安装元目录引擎和服务驱动程序。在 NetWare 平台上，这些包括 Identity Manager Drivers for Avaya、 eDirectory™、 GroupWise®、 JDBC*、 JMS*、 LDAP、Linux/UNIX 设置、RACF*、SOAP、SIF*、Top Secret 和 Work Order。选择该选项还会扩展 eDirectory 纲要。

  重要：必须先安装带最新增补程序的 Novell eDirectory 8.7.3.6 或更高版本和 Security Services 2.0.5 (NMAS™ 3.1.3)，之后才能安装此选项。如果要运行 Identity Manager 的元目录引擎，请安装元目录服务器组件。如果 NMAS 的版本不正确，将收到警报讯息，并将丢失 Identity Manager 功能。

- **已连接系统：**安装 Remote Loader，用于在已连接系统和运行元目录引擎的服务器之间建立链接。

  对于在 Netware 上安装 Identity Manager，该选项不可用，“安装”屏幕上看不到此选项。

- **Identity Manager 万维网组件：**该选项将安装 Identity Manager 插件和驱动程序配置。

  只有在安装 Novell iManager 后才能安装该选项。

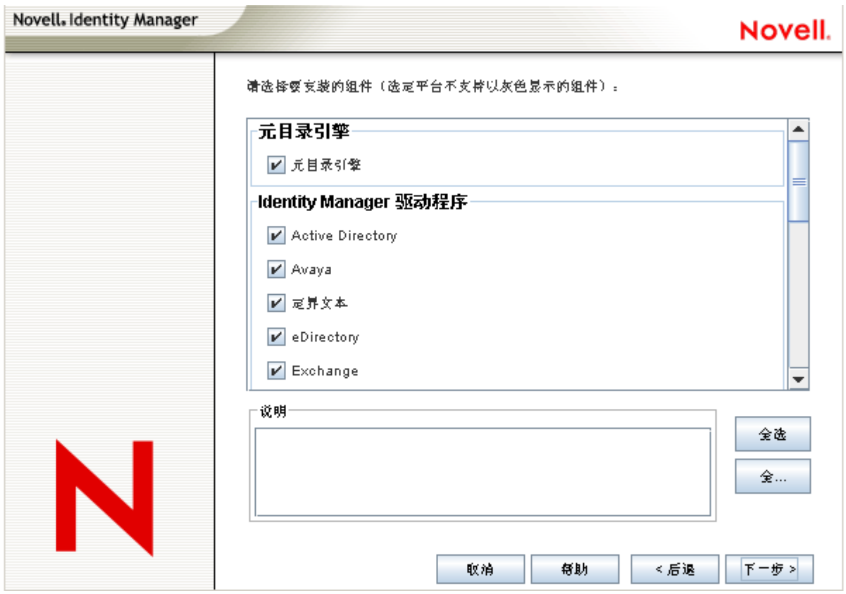
- **实用程序：**安装 JDBC 驱动程序的其他底稿，以及其他驱动程序的实用程序。大多数驱动程序没有与其相连的实用程序。驱动程序实用程序可以包含：
  - 用于 JDBC 驱动程序的 SQL 底稿
  - JMS 组件
  - PeopleSoft 组件
  - 许可证审计工具
  - Active Directory 发现工具
  - Lotus Notes 发现工具

- SAP 实用程序

通过另一个实用程序，可以注册用于 Identity Manager 的 Novell Audit Systerm 组件（在安装此实用工具之前，必须在树上安装有效的 eDirectory 版本和 Novell Audit 日记记录服务器）。

10 单击 *下一步*。

11 选择要安装的驱动程序，然后单击 *下一步*。



“选择安装引擎的驱动程序”页显示可以在相应平台上安装哪些驱动程序。例如，在 NetWare 服务器上，无法安装 Windows Active Directory 驱动程序。

默认情况下，将选中此选项所有可用的驱动程序。建议安装所有选定的驱动程序文件，这样，如果以后想要另一个驱动程序，就不需要运行安装程序。通过 iManager 或 Designer 配置驱动程序且将其部署之前，不使用这些驱动程序文件。

如果不想安装所有驱动程序，则可以单击 *全部清除*，然后选择需要的驱动程序，也可以单击不想安装的驱动程序以取消选择这些驱动程序。如果以后需要其他驱动程序，您将需要重新运行此安装程序以安装没有选择的任何驱动程序。还可以使用 Designer 来创建、修改和部署驱动程序文件。

12 当看到有关产品激活的提示讯息时，单击 *确定*。

需要在安装驱动程序后的 90 天内激活，否则它们将会关闭。

13 在 “纲要扩展”页上，指定下列项目：



- **用户名：**指定有权扩展纲要的用户的用户名 （使用 LDAP 格式，例如 CN=admin,O=novell）。在此页上，选择具有足够权限扩展 eDirectory 纲要的用户 （对树的根具有主管权限的用户，比如 Admin）。
- **用户口令 :** 指定用户的口令。

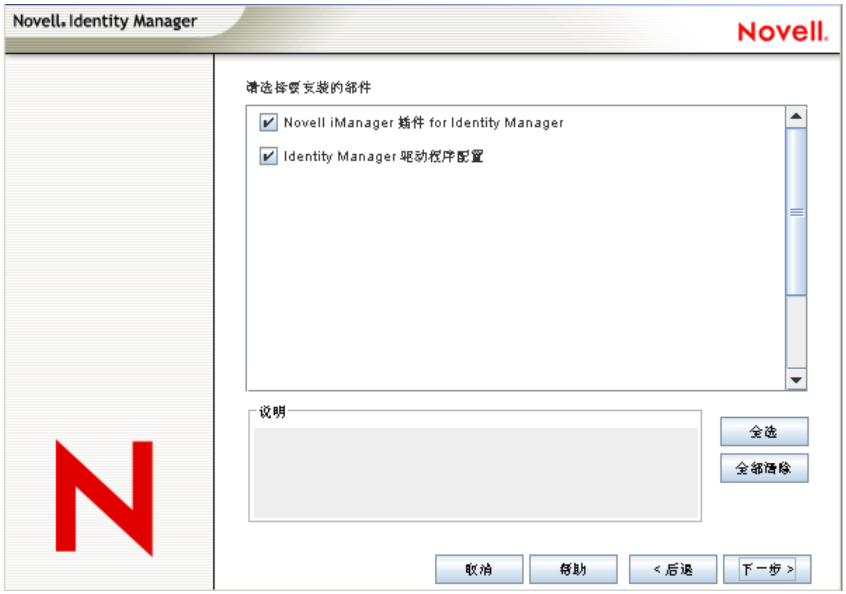
14 单击 *下一步*。

验证用户信息后，将显示第一个 （共两个）“组件”页。

在第一个 “组件”页上，如果在服务器上安装了 Novell Audit 系统，则 *Identity Manager 的 Novell Audit 系统组件*将被选中。否则，将不选择该项。*应用程序组件*选项用于安装 JDBC 和 PeopleSoft 等应用程序系统的组件。

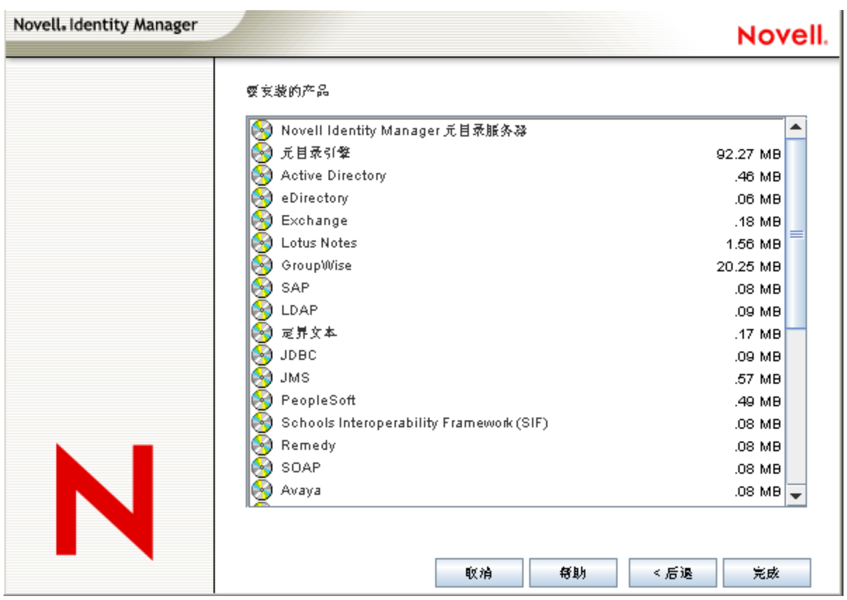
如果安装程序检测到现有驱动程序配置文件，会将其移至一个备份路径。

15 单击*下一步*。



16 第二个 “组件”页用于安装实用程序。如果特定于平台的实用程序不可用于执行安装的平台，则这些实用程序将会显示为灰色。对于 NetWare，唯一可用的选项是 “用于 JDBC 驱动程序和 JMS 组件的 SQL 底稿”。选择需要的组件，然后单击*下一步*。

17 阅读并确认 “摘要”页上的选项，然后单击*完成*。



Novell Identity Manager 安装过程将关闭 eDirectory 以扩展纲要。安装过程开始安装选定的产品和组件。



18 安装完成并显示 “安装完成”对话框后，单击*关闭*。

19 为使 iManager 识别安装的插件，请立即重新启动万维网服务并重新启动 Tomcat。

如果已安装了 Identity Manager 驱动程序，可以使用 iManager 2.6 或更高版本中的 Identity Manager 配置向导或使用 Designer 来配置驱动程序。

4.4 在 Windows 上安装 Identity Manager

该过程包括适用于 Windows 的 元目录服务器、万维网组件和实用程序的安装。

开始之前，请确保系统符合表 1-3 （第 28 页）中列出的要求。

1 下载所需的 Identity Manager .iso 映像文件。可以从 Novell 下载站点下载 Identity Manager .iso (http://download.novell.com) 映像文件。

Identity Manager 的 Windows 安装位于 Identity_Manager_3_5_1_NW_Win.iso 或 Identity_Manager_3_5_1_DVD.iso 上。

2 解压文件之后，请双击 \NT 目录中的 install.exe 文件。

完成文件的复制后，将显示 “Identity Manager 产品安装”页。



3 单击 *下一步*开始安装。

4 选择查看许可证协议的语言，或者使用默认语言 （英语）。

Identity Manager 安装程序将自动以安装程序的计算机上所使用的语言运行。如果安装程序没有被翻译为该计算机所使用的语言，则默认使用英语。

5 阅读许可证协议，然后单击*我接受*。

6 查看说明系统类型 （包括 “元目录服务器”、“万维网组件”和 “实用程序”）的 “概述”页，然后单击 *下一步*继续。

表 1-3 （第 28 页）也对此信息进行了说明。

7 在 “Identity Manager 安装” 页上，选择要安装的组件：



下列选项可用：

- **元目录服务器：**安装元目录引擎和服务驱动程序。这些包括 Identity Manager Drivers for Active Directory、 Avaya、 Delimited Text、 eDirectory、 Exchange、 GroupWise、 JDBC、 JMS、 LDAP、 Linux/UNIX 设置、 Lotus Notes、 PeopleSoft、 RACF、Remedy、SOAP、SAP、SIF 和 Top Secret。选择该选项还会扩展 eDirectory 纲要。

  重要：必须先安装带最新增补程序的 Novell eDirectory 8.7.3.6 或 8.8 和 Security Services 2.0.5 (NMAS 3.1.3)，之后才能安装此选项。如果要运行 Identity Manager 的元目录引擎，请安装元目录服务器组件。如果 NMAS 的版本不正确，将收到警报讯息，并将丢失 Identity Manager 功能。

- **已连接系统：**安装 Remote Loader，用于在已连接系统和运行元目录引擎的服务器之间建立链接。对于 Windows，此选项安装以下驱动程序：Active Directory、Avaya、Delimited Text、eDirectory、Exchange、GroupWise、JDBC、JMS、LDAP、Linux/UNIX 设置、Lotus Notes、PeopleSoft、RACF、Remedy、SOAP、SAP、SIF 和 Top Secret。

  安装已连接系统，使应用程序能够从应用程序服务器连接到运行元目录引擎的基于 eDirectory 的服务器。中包括该过程。第 4.5 节 “在 Windows 上安装已连接系统选项”（第 75 页）

- **万维网组件：**该选项用于安装驱动程序配置、 iManager 插件、应用程序底稿和实用程序。

  只有在安装 Novell iManager 后才能安装该选项。

- **实用程序：**安装 JDBC 驱动程序的其他底稿，以及其他驱动程序的实用程序。大多数驱动程序没有与其相连的实用程序。驱动程序实用程序可以包含：
  - 用于 JDBC 驱动程序的 SQL 底稿
  - JMS 组件

- PeopleSoft 组件
- 许可证审计工具
- Active Directory 发现工具
- Lotus Notes 发现工具
- SAP 实用程序
- 脚本编写驱动程序安装程序和配置工具

通过另一个实用程序，可以注册用于 Identity Manager 的 Novell Audit Systerm 组件（在安装此实用工具之前，必须在树上安装有效的 eDirectory 版本和 Novell Audit 日记记录服务器）。

8 单击 *下一步*。

9 选择要安装的驱动程序，然后单击 *下一步*。



"选择安装引擎的驱动程序"页显示可以在相应平台上安装哪些驱动程序。默认情况下，将选择所有可用的驱动程序。

建议安装所有选定的驱动程序文件，这样，如果以后想要另一个驱动程序，就不需要运行安装程序。通过 iManager 或 Designer 配置驱动程序之前，不使用这些驱动程序文件。

10 当看到有关产品激活的提示讯息时，单击 *确定*。

需要在安装驱动程序后的 90 天内激活，否则它们将会关闭。

11 当看到"口令同步升级警告！"讯息时，单击 *确定*。

此讯息适用于运行 Password Synchronization 1.0 的 Windows 服务器。如果希望版本 1.0 具有向后兼容性，则必须对驱动程序配置文件添加额外的策略。如果没有这些策略，则 Password Synchronization 1.0 只对现有帐户起作用，而对新帐户或重命名的帐户不起作用。

12 在 “纲要扩展”页上，指定下列项目：



- **用户名：** 指定有权扩展 eDirectory 纲要的用户 （对 Tree 的 Root 具有主管权限的用户，比如 Admin）的用户名 （用 LDAP 格式，如 CN=admin,O=novell）。
- **用户口令 :** 指定用户的口令。

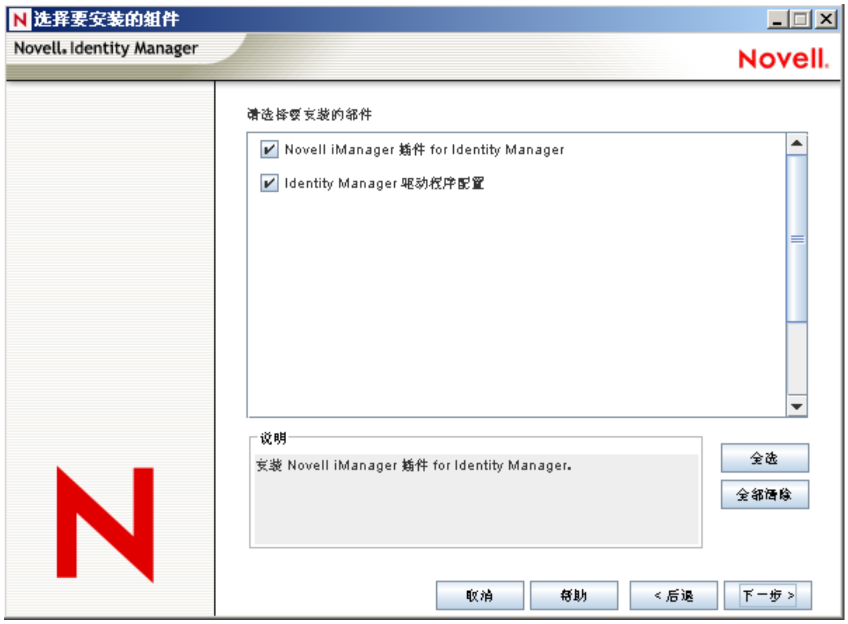
13 单击*下一步*。验证用户信息后，将显示第一个 （共两个）“组件”页：

如果在树上安装有有效版本的 eDirectory 和 Novell Audit 日志记录服务器，则 “选择要安装的组件”页上的*注册 Identity Manager 的 Novell Audit 系统组件*将被选中。否则，不选中该选项。*应用程序组件*选项用于安装 JDBC 和 PeopleSoft 等应用程序系统的组件。

如果安装程序检测到现有驱动程序配置文件，会将其移至一个备份路径。

Client Login Extension for Novell Identity Manager 选项会将 Client Login Extension 的安装程序复制到您的文件系统。要获取有关 Client Login Extension for Novell Identity Manager 的更多信息，请参阅 《*Novell Identity Manager 3.5.1 管理指南*》中的 “Client Login Extension for Novell Identity Manager 3.5.1”。

14 选择要安装的组件，然后单击*下一步*。



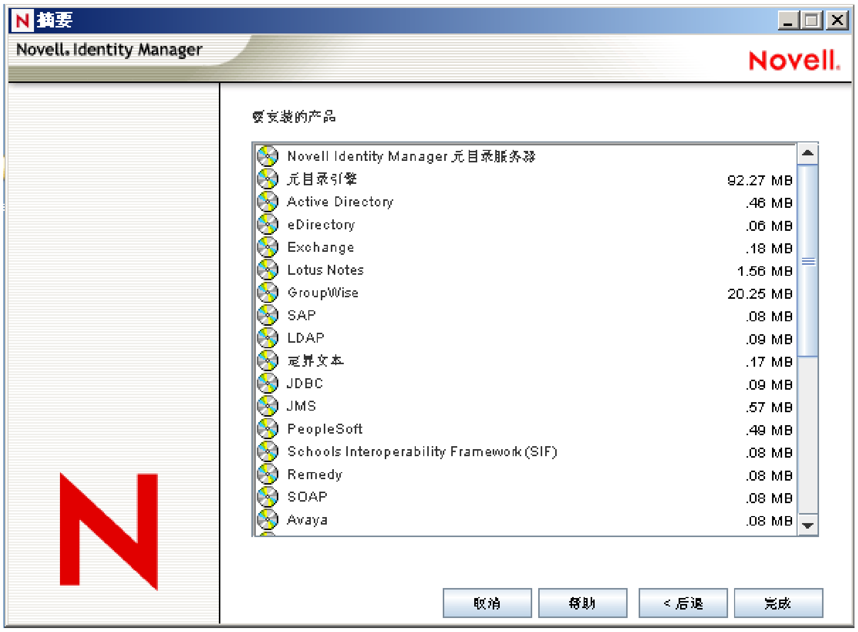
15 将另外显示一个页面，用于安装 iManager 的 Identity Manager 插件，使用 SSL 端口 443。单击*下一步*。

16 第二个 “组件”页用于安装实用程序。 Windows 安装将出现另一个屏幕，其中显示放置应用程序组件的目录。默认目录为 C:\Novell\NDS\DirXMLUtilities。单击*下一步*。

17 在 “选择要安装的组件”页上，如果特定于平台的实用程序不可用于执行安装的平台，则这些实用程序将会显示为灰色。对于 Windows，所有组件均可用，这些组件包括用于 JDBC 驱动程序的 SQL 底稿、 JMS 组件、 PeopleSoft 组件、许可证审计工具、 Active Directory 发现工具、 Lotus Notes 发现工具、 SAP 实用程序和脚本编写驱动程序安装程序和配置工具。选择需要的组件，然后单击*下一步*。

18 如果选择将 Client Login Extension for Novell Identity Manager 的安装程序复制到文件系统，请选择安装路径或使用默认路径 C:\Novell\NDS\DirXMLUtilities\cle。单击*下一步*。

19 阅读并确认 “摘要”页上的选项，然后单击*完成*。



Novell Identity Manager 安装过程将关闭 eDirectory 以扩展纲要。安装过程开始安装选定的产品和组件。

20 安装完成并显示 “安装完成”对话框后，单击*关闭*。

21 为使 iManager 识别安装的插件，请立即重新启动万维网服务并重新启动 Tomcat。

如果已安装了 Identity Manager 驱动程序，可以使用 iManager 2.6 或更高版本中的 Identity Manager 配置向导或使用 Designer 来配置驱动程序。

4.5 在 Windows 上安装已连接系统选项

第 4.4 节 “在 Windows 上安装 Identity Manager”（第 69 页）包括用于 Windows 的元目录服务器、万维网组件和实用程序的安装。此外， Windows 服务器可以使用 “已连接系统”选项。

如果不希望将 eDirectory 服务和元目录引擎的开销施加到应用程序服务器，请使用 “已连接系统”选项。使用 Remote Loader，就可以通过 Identity Manager 实现所需的同步，而不需要装载从其他位置即可访问的应用程序。

开始之前，请确保系统符合表 1-3 （第 28 页）中列出的要求。

1 下载所需的 Identity Manager .iso 映像文件。可以从 Novell 下载站点下载 Identity Manager .iso (http://download.novell.com) 映像文件。

Identity Manager 的 Windows 安装位于 Identity_Manager_3_5_1_NW_Win.iso 或 Identity_Manager_3_5_1_DVD.iso 上。

2 运行 \NT 目录中的 install.exe。

3 阅读欢迎信息，然后单击 *下一步*。

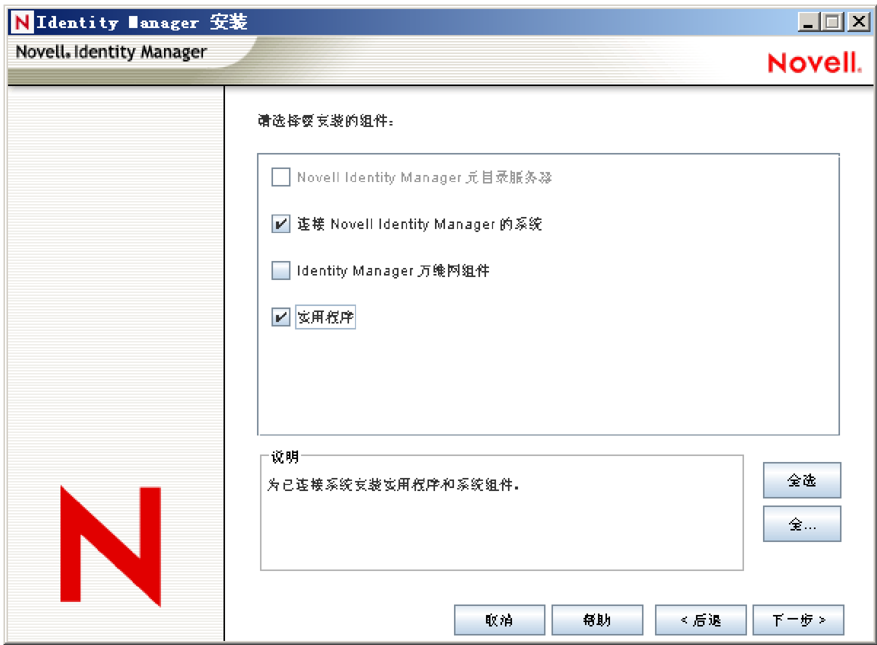
4 选择查看许可证协议的语言，或者使用默认语言 （英语）。

Identity Manager 安装程序将自动以安装程序的计算机上所使用的语言运行。如果安装程序没有被翻译为该计算机所使用的语言，则默认使用英语。

5 阅读许可证协议，然后单击*我接受*。

6 查看有关各个系统和组件的 “概述”页，然后单击 *下一步*开始安装。

7 要选择 “已连接系统”选项，请首先单击*全部清除*，然后选择*已连接系统*和*实用程序*。如果在此服务器上安装了 iManager 实用程序，并且需要添加 Identity Manager 的 Identity Manager 插件以及驱动程序配置，则还应选择*万维网组件*。

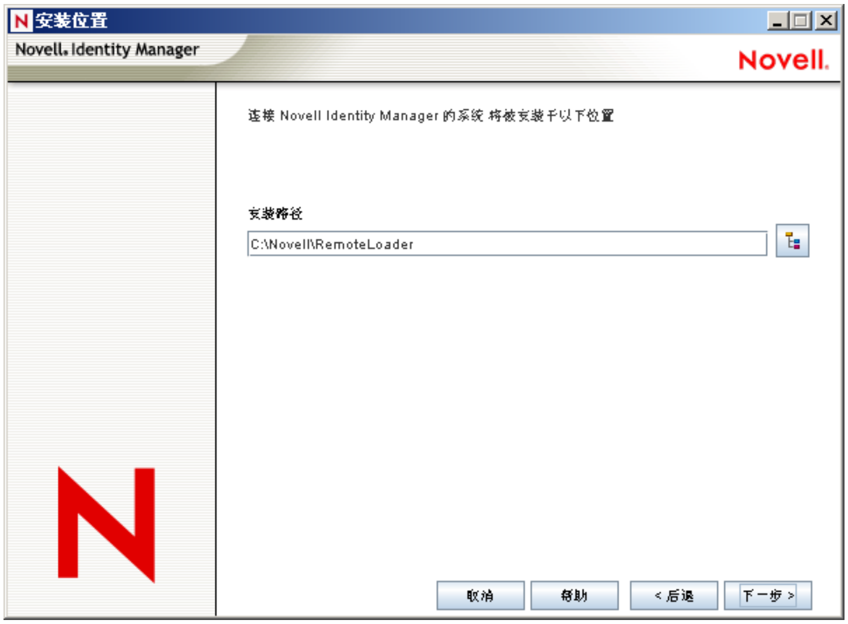


- **已连接系统：**安装 Remote Loader，用于在已连接系统和运行元目录引擎的服务器之间建立链接。对于 Windows，此选项安装以下驱动程序：Active Directory、Avaya、Delimited Text、eDirectory、Exchange、GroupWise、JDBC、JMS、LDAP、Linux/UNIX 设置、Lotus Notes、PeopleSoft、RACF、Remedy、SOAP、SAP、SIF 和 Top Secret。
- **实用程序：**安装 JDBC 驱动程序的其他底稿，以及其他驱动程序的实用程序。大多数驱动程序没有与其相连的实用程序。驱动程序实用程序可以包含：
  - 用于 JDBC 驱动程序的 SQL 底稿
  - JMS 组件
  - PeopleSoft 组件
  - 许可证审计工具
  - Active Directory 发现工具
  - Lotus Notes 发现工具
  - SAP 实用程序
  - 脚本编写驱动程序安装程序和配置工具

  通过另一个实用程序，可以注册用于 Identity Manager 的 Novell Audit Systerm 组件（在安装此实用工具之前，必须在树上安装有效的 eDirectory 版本和 Novell Audit 日记记录服务器）。

8 单击 *下一步*。

9 在 “安装位置”页上，单击 *下一步*接受默认的目录路径，即 C:\Novell\RemoteLoader。



10 在“选择用于安装 Remote Loader 的驱动程序”页上，选择需要装载的 Identity Manager 驱动程序，然后单击 *下一步*。



驱动程序选项包括 Active Directory、 Avaya、 Delimited Text、 eDirectory、 Exchange、 Groupwise、 JDBC、 JMS、 LDAP、 Linux/UNIX 设置、 Lotus Notes、 PeopleSoft、 RACF、 Remedy、 SOAP、 SAP、 SIF 和 Top Secret。

如果不想安装所有驱动程序，则可以单击*全部清除*，然后选择需要的驱动程序，也可以单击不想安装的驱动程序以取消选择这些驱动程序。如果以后需要其他驱动程序，您将

需要重新运行此安装程序以安装没有选择的任何驱动程序。还可以使用 Designer 来创建、修改和部署驱动程序文件。

11 当看到有关产品激活的提示讯息时，单击*确定*。

需要在安装驱动程序后的 90 天内激活，否则它们将会关闭。

12 当看到 “口令同步升级警告！ ” 讯息时，单击*确定*。

此讯息适用于运行 Password Synchronization 1.0 的 Windows 服务器。如果希望版本 1.0 具有向后兼容性，则必须对驱动程序配置文件添加额外的策略。如果没有这些策略，则 Password Synchronization 1.0 只对现有帐户起作用，而对新帐户或重命名的帐户不起作用。

13 单击*是*可在桌面上创建 Remote Loader 控制台的快捷方式。如果不想创建快捷方式，请单击*否*。

如果在树上安装有有效版本的 eDirectory 和 Novell Audit 日志记录服务器，则 “选择要安装的组件”页上的*注册 Identity Manager 的 Novell Audit 系统组件*将被选中。否则，不选中该选项。*应用程序组件*选项用于安装 JDBC 和 PeopleSoft 等应用程序系统的组件。

Client Login Extension for Novell Identity Manager 选项会将 Client Login Extension 的安装程序复制到您的文件系统。要获取有关 Client Login Extension for Novell Identity Manager 的更多信息，请参阅 《*Novell Identity Manager 3.5.1 管理指南*》中的 “Client Login Extension for Novell Identity Manager 3.5.1”。

14 选择要安装的组件，然后单击 *下一步*。

15 单击 *下一步*接受 Identity Manager 实用程序的默认安装路径（C:\Novell\NDS\DirXMLUtilities）。

16 选择要安装的驱动程序组件和实用程序，然后单击 *下一步*。



17 如果选择将 Client Login Extension for Novell Identity Manager 的安装程序复制到文件系统，请选择安装路径或使用默认路径 C:\Novell\NDS\DirXMLUtilities\cle。单击 *下一步*。

18 查看 “摘要”页列出的项目。如果认可，请单击*完成*以安装组件。

19 单击*关闭*退出安装程序。

4.6 在 UNIX/Linux 平台上通过 GUI 界面安装 Identity Manager

开始之前，请确保系统符合第 4.2 节 “Identity Manager 组件和系统要求”（第 63 页）中列出的要求。

1 下载所需的 Identity Manager .iso 映像文件。可以从 Novell 下载站点下载 Identity Manager .iso (http://download.novell.com) 映像文件。

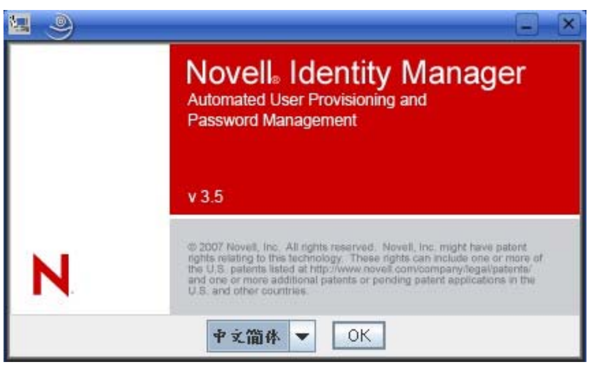
例如， Identity Manager 的 Linux 安装位于 Identity_Manager_3_5_1_Linux.iso 或 Identity_Manager_3_5_1_DVD.iso 上，而 AIX 和 Solaris 位于 Identity_Manager_3_5_1_Unix.iso 或 Identity_Manager_3_5_1_DVD.iso 上。

2 在主机上，请以 root 用户身份登录。

3 要在 Linux 上运行 GUI 安装，请单击根目录中的 install.bin 文件。将询问是要以终端模式还是显示模式运行安装文件。选择*终端*。install.bin 将检查 Xwindows 是否存在，如果存在，将启动用于 Linux 的 Identity Manager 的 GUI 安装程序。

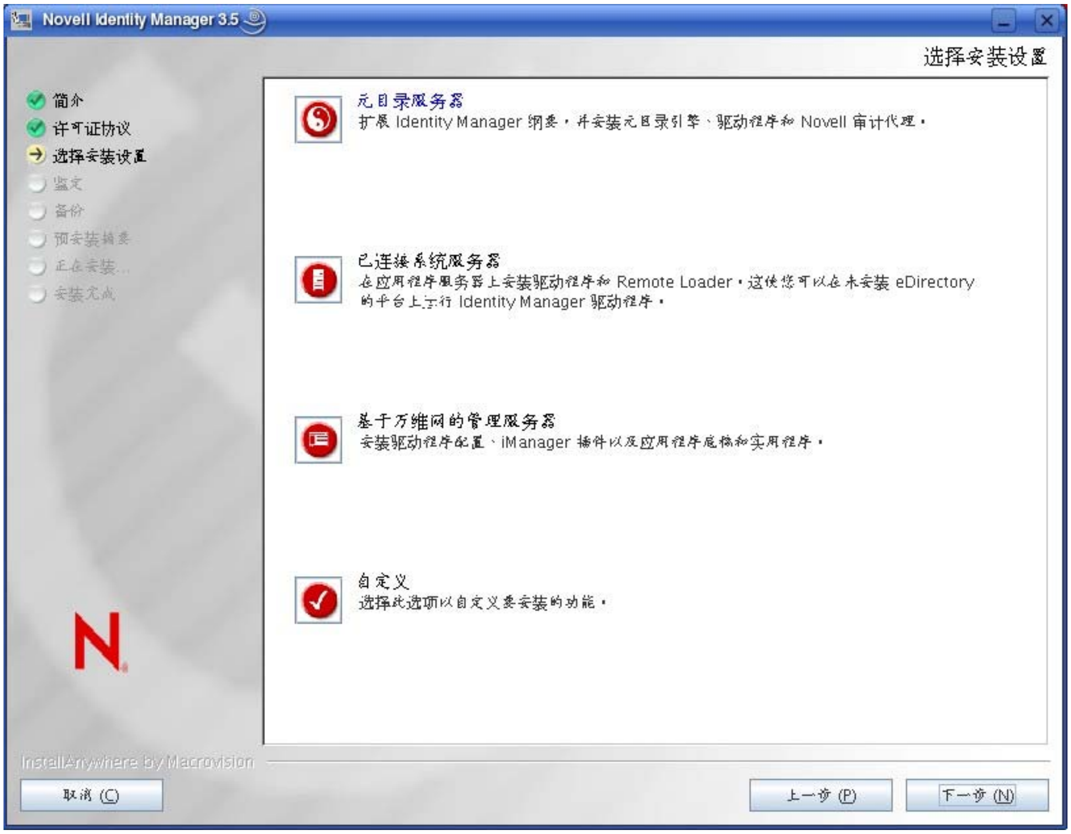
注释：如果单击 install.bin 后没有启动 GUI 安装程序，请打开终端窗口并手动运行 install.bin。如果在 Solaris 服务器上运行 eDirectory 8.8.x，则不要通过 GUI 运行 Identity Manager 安装程序。请参见第 4.7 节 “在 UNIX/Linux 平台上使用控制台安装 Identity Manager”（第 83 页）。

4 选择运行安装程序要使用的语言，或使用默认语言 （英语）。单击*确定*。



5 查看欢迎信息，然后单击 *下一步*继续安装。

6 阅读许可证协议，选择*我接受许可证协议中的条款*，然后单击*下一步*。



7 指定要安装的安装集。安装集包含下列组件：

- **元目录服务器：**安装元目录引擎和服务驱动程序、 Identity Manager 驱动程序、 Novell Audit 代理，并扩展 eDirectory 纲要。

  必须先安装带最新 Support Pack 的 Novell eDirectory 8.7.3.6 或更高版本和 Security Services 2.0.5 (NMAS 3.1.3)，之后才能安装此选项。如果这些未安装，则 Identity Manager 安装进程将终止。

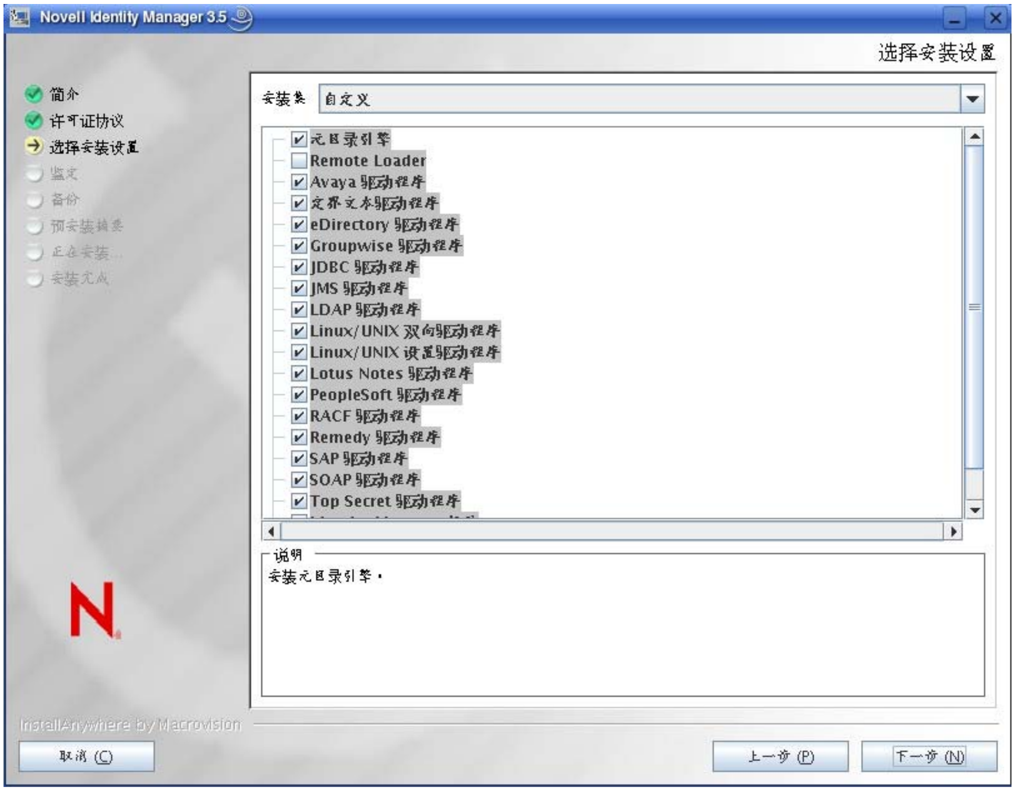
- **已连接系统服务器：**安装 Remote Loader 和以下驱动程序：Avaya、 Delimited Text、 GroupWise、 JDBC、 JMS、 LDAP、 Linux/UNIX 设置、 Linux/UNIX Bidirectional、 Lotus Notes、PeopleSoft、RACF、Remedy、SAP、SIF、Top Secret 和 Work Order。如果不希望将 eDirectory 服务和元目录引擎的开销加到应用程序服务器，请使用 “已连接系统服务器”选项。

- **基于万维网的管理服务器：**安装 Identity Manager 插件和 Identity Manager 驱动程序策略。

  只有在安装 Novell iManager 后才能安装该选项。

  默认情况下， Linux/UNIX 安装中不安装 Identity Manager 驱动程序实用程序。要安装的话，必须手动将实用程序从 Identity Manager 安装 CD 复制到 Identity Manager 服务器。所有实用程序均位于*平台的* \setup\utilities 目录中。

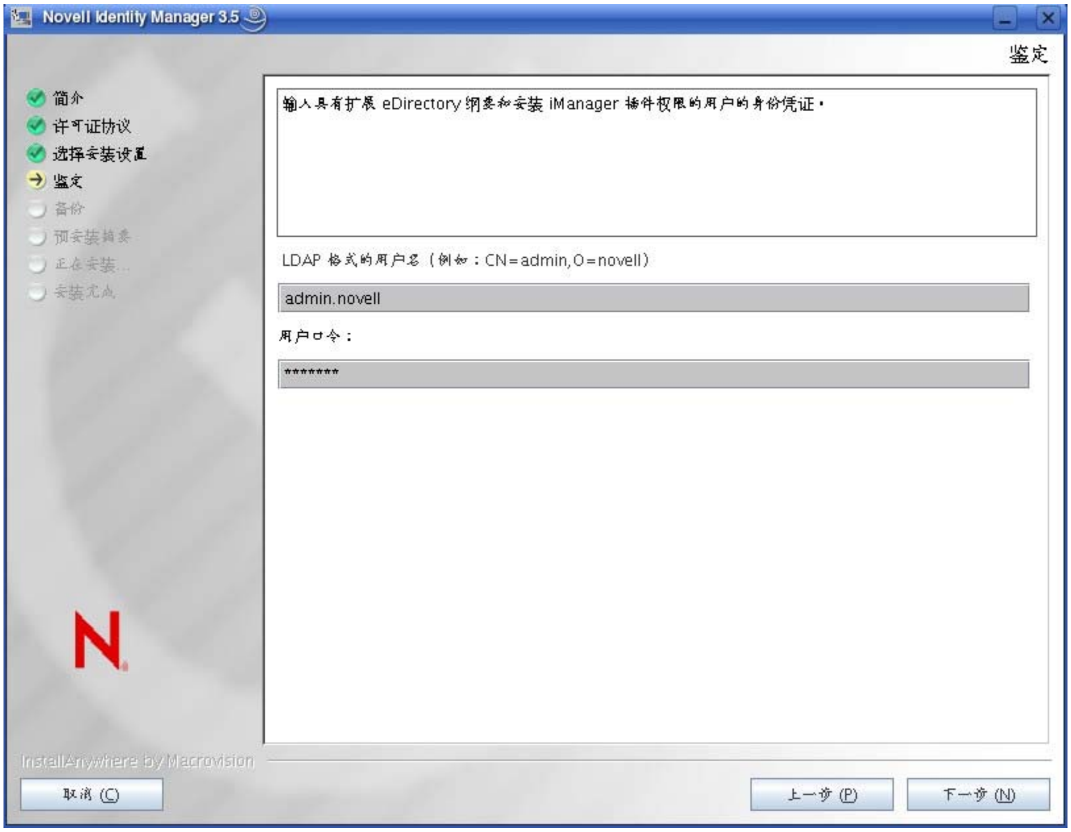
- **自定义：**安装从所有组件的列表中选择的特定组件。



可以通过选择*上一步*返回前面的菜单并修改安装选项。

8 （可选）根据选择的选项（比如元目录服务器）以及是否正在运行 eDirectory v8.8，提示设置 LD_LIBRARY_PATH 环境变量。要实现这一点，通过输入 . /opt/novell/eDirectory/bin/ndspath, 执行 /opt/novell/eDirectory/bin/ndspath 底稿，然后重新运行安装。

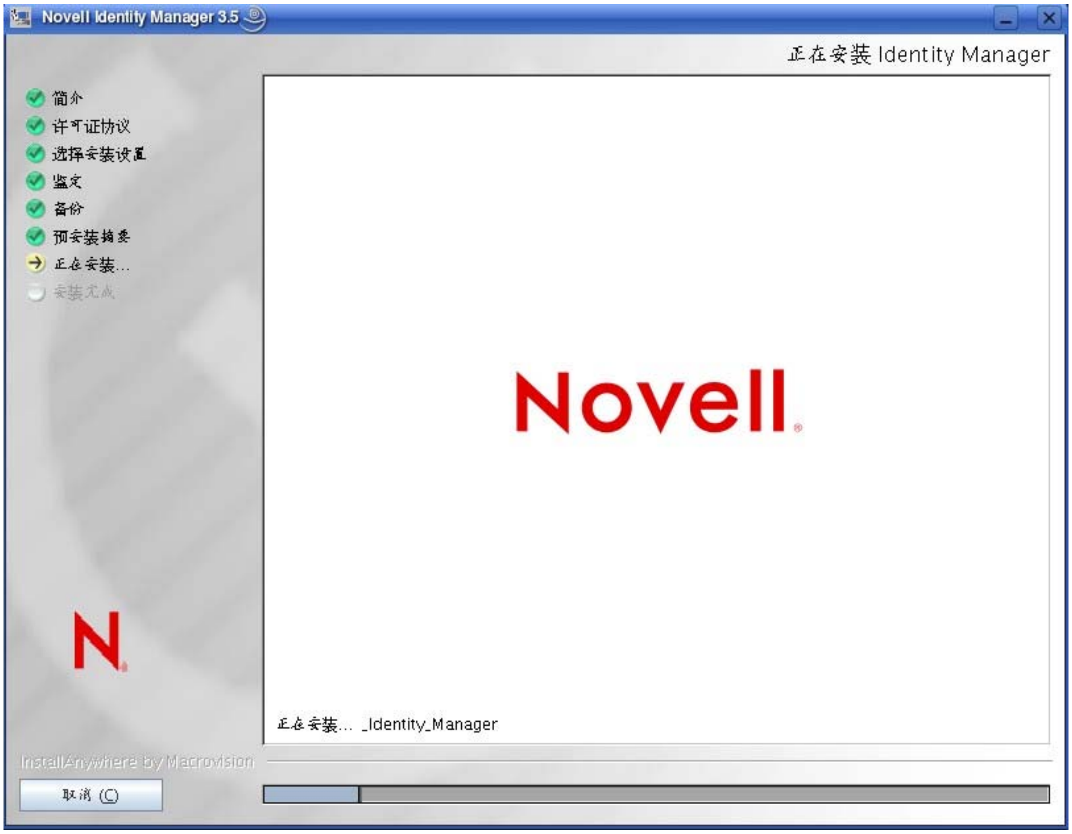
9 如果选择安装 元目录服务器，则系统会提示您提供 LDAP 用户名 (CN=admin,O=novell) 和口令。选择具有足够权限扩展 eDirectory 纲要的用户 （对树的根具有主管权限的用户，比如 Admin）。



重要：（仅对于 Solaris 安装）如果要在 eDirectory 驻留的同一服务器上安装基于万维网的管理服务器，当提示询问万维网服务器的安全端口时，请将默认值更改为某个空闲端口，比如 8443。

---

10 校验 “安装前摘要”页上的信息是否正确，然后单击*安装*开始安装包。



安装元目录引擎和纲要文件时， eDirectory 将暂时关闭。默认情况下，将安装所有可用的驱动程序，这样，如果以后想要另一个驱动程序，就不需要运行安装程序。通过 iManager 或 Designer 配置驱动程序且将其部署之前，不使用这些驱动程序文件。

11 当看到 “安装完成”页面时，单击*完成*关闭安装程序。

4.7 在 UNIX/Linux 平台上使用控制台安装 Identity Manager

开始之前，请确保系统符合表 1-3 （第 28 页）中列出的要求。

1 下载所需的 Identity Manager .iso 映像文件。可以从 Novell 下载站点下载 Identity Manager .iso (http://download.novell.com) 映像文件。

例如， Identity Manager 的 Linux 安装位于 Identity_Manager_3_5_1_Linux.iso 或 Identity_Manager_3_5_1_DVD.iso 上，而 AIX 和 Solaris 位于 Identity_Manager_3_5_1_Unix.iso 或 Identity_Manager_3_5_1_DVD.iso 上。

2 在主机上，请以 root 用户身份登录。

3 执行安装目录中的 .bin 文件。

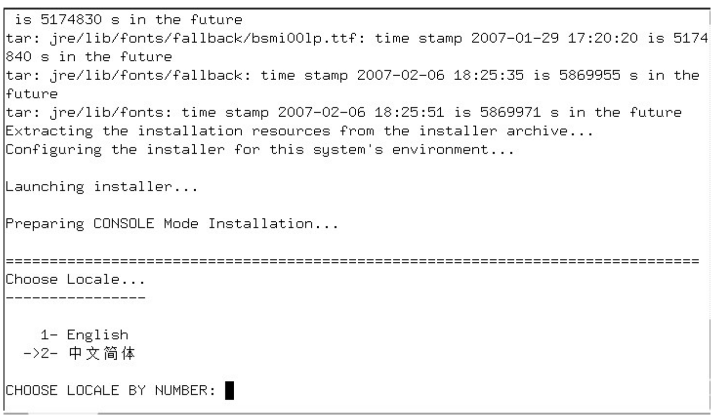
将当前工作目录更改为安装目录，即安装所在的位置。然后输入下列命令之一，以运行安装。

平台	示例路径	安装文件
Linux	linux/setup/	idm_linux.bin
Solaris	solaris/setup/	idm_solaris.bin
AIX	aix/setup/	idm_aix.bin

这些路径是安装映像根的相对路径，可能是展开此映像或装入 CD 的位置。这也取决于所下载的 ISO 映像。例如， Linux 位于 Identity_Manager_3_5_1_Linux.iso 或 Identity_Manager_3_5_1_DVD.iso 上，而 AIX 和 Solaris 位于 Identity_Manager_3_5_1_Unix.iso 或 Identity_Manager_3_5_1_DVD.iso 上。

除非当前工作目录是安装程序所在的目录，否则安装程序将无法找到要安装的程序包。

4 选择运行安装程序要使用的语言，或使用默认语言 （英语）。键入一个编号，然后按 Enter 键。



```
 is 5174830 s in the future
tar: jre/lib/fonts/fallback/bsmi00lp.ttf: time stamp 2007-01-29 17:20:20 is 5174
840 s in the future
tar: jre/lib/fonts/fallback: time stamp 2007-02-06 18:25:35 is 5869955 s in the
future
tar: jre/lib/fonts: time stamp 2007-02-06 18:25:51 is 5869971 s in the future
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...

Launching installer...

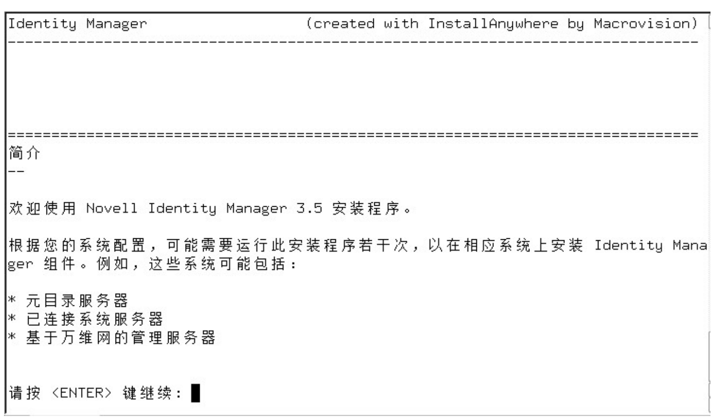
Preparing CONSOLE Mode Installation...

===============================================================================
Choose Locale...
----------------

    1- English
  ->2- 中文简体

CHOOSE LOCALE BY NUMBER:
```

5 查看欢迎信息，然后按 Enter 键继续安装。



```
Identity Manager                  (created with InstallAnywhere by Macrovision)
-------------------------------------------------------------------------------




===============================================================================
简介
--

欢迎使用 Novell Identity Manager 3.5 安装程序。

根据您的系统配置，可能需要运行此安装程序若干次，以在相应系统上安装 Identity Mana
ger 组件。例如，这些系统可能包括：

* 元目录服务器
* 已连接系统服务器
* 基于万维网的管理服务器


请按 <ENTER> 键继续：
```

6 按 Enter 键浏览许可证协议，如果同意这些使用条款，请输入 Y。如果不同意，请输入 N 退出安装程序。

```
===============================================================================
选择安装设置
------

请选取将由本安装程序安装的"安装集"。

  ->1- 元目录服务器
    2- 已连接系统服务器
    3- 基于万维网的管理服务器

    4- 定制...

针对所选"安装集"输入相应的号码，或按一下 <ENTER> 接受默认值
      :
```

7 指定要安装的安装集的相应编号 (1-4)。安装集包含下列组件：

- **1 一 元目录服务器：**安装元目录引擎和服务驱动程序、Identity Manager 驱动程序、Novell Audit 代理，并扩展 eDirectory 纲要。

  必须先安装带最新 Support Pack 的 Novell eDirectory 8.8 或 8.8 和 Security Services 2.0.5 (NMAS 3.1.3)，之后才能安装此选项。如果未安装这些软件，Identity Manager 安装进程将终止。
- **2 一 已连接系统服务器：**安装 Remote Loader 和以下驱动程序：Avaya、 Delimited Text、 GroupWise、 JDBC、 JMS、 LDAP、 Linux/UNIX 设置、 Linux/UNIX Bidirectional、 Lotus Notes、 PeopleSoft、 RACF、 Remedy、 SAP、 SIF、 Top Secret 和 Work Order。如果不希望将 edirectory 服务和 元目录引擎的开销加到应用程序服务器，请使用*已连接系统*选项。
- **3 一 基于万维网的管理服务器：**安装 Identity Manager 插件和 Identity Manager 驱动程序策略。

  只有在安装 Novell iManager 后才能安装该选项。

  默认情况下， Linux/UNIX 安装中不安装 Identity Manager 驱动程序实用程序。要安装的话，必须手动将实用程序从 Identity Manager 安装 CD 复制到 Identity Manager 服务器。所有实用程序均位于*平台的* \setup\utilities 目录中。
- **4 - 自定义：**安装从所有组件的列表中选择的特定组件。

```
安装集
    元目录服务器

产品组件：
    SAP 驱动程序,
    eDirectory 驱动程序,
    LDAP 驱动程序,
    元目录引擎,
    JDBC 驱动程序,
    定界文本驱动程序,
    Lotus Notes 驱动程序,
    Groupwise 驱动程序,
    Avaya 驱动程序,
    SOAP 驱动程序,
    Remedy 驱动程序,
    PeopleSoft 驱动程序,
    JMS 驱动程序,
    Linux/UNIX 双向驱动程序,
    Linux/UNIX 设置驱动程序,
    RACF 驱动程序,
    Top Secret 驱动程序


请按 <ENTER> 键继续：
```

可以通过输入 prev 返回前面的菜单并修改安装选项。

8 （可选）根据选择的选项 （比如元目录服务器）以及是否正在运行 eDirectory v8.8，提示设置 LD_LIBRARY_PATH 环境变量。要选择功能，请通过键入 ./opt/novell/eDirectory/bin/dspath 执行 /opt/novell/eDirectory/bin/ndspath 底稿，然后重新运行安装。

9 如果选择安装 元目录服务器，则系统会提示您提供 LDAP 用户名 (CN=admin,O=novell) 和口令。选择具有足够权限扩展 eDirectory 纲要的用户 （对树的根具有主管权限的用户，比如 Admin）。

重要：（仅对于 Solaris 安装）如果要在 eDirectory 驻留的同一服务器上安装基于万维网的管理服务器，当提示询问万维网服务器的安全端口时，请将默认值更改为某个空闲端口，比如 8443。

---

10 校验摘要中包含的信息是否正确，然后按 Enter 键开始安装包。

```
===========================================================================
正在安装...
-------

 [==================|==================|==================|==================]
 [------------------|------------------|------------------|------------------]


===========================================================================
安装完成
----

恭喜。Novell Identity Manager 3.5 已经成功安装到您的系统中。

如果已经安装了 Identity Manager 插件，请重启动应用程序服务器。

按一下 <ENTER> 键退出安装程序：
```

安装元目录引擎和纲要文件时， eDirectory 将暂时关闭。默认情况下，将安装所有可用的驱动程序，这样，如果以后想要另一个驱动程序，就不需要运行安装程序。通过 iManager 或 Designer 配置驱动程序且将其部署之前，不使用这些驱动程序文件。

11 当看到 “安装完成”屏幕时，按 Enter 键关闭安装程序。

4.8 在 UNIX/Linux 上使用控制台安装已连接系统选项

第 4.7 节 “在 UNIX/Linux 平台上使用控制台安装 Identity Manager”（第 83 页）包括 UNIX 平台上的元目录服务器、万维网组件和实用程序的安装。此外， UNIX 或 Linux 服务器可以使用 “已连接系统”选项。

如果不希望将 eDirectory 服务和元目录引擎的开销加到应用程序服务器，请使用 “已连接系统”选项。使用 Remote Loader，就可以通过 Identity Manager 实现所需的同步，而不需要装载从其他位置即可访问的应用程序。

开始之前，请确保系统符合表 1-3 （第 28 页）中列出的要求。

1 下载所需的 Identity Manager .iso 映像文件。可以从 Novell 下载站点下载 Identity Manager .iso (http://download.novell.com) 映像文件。

例如， Identity Manager 的 Linux 安装位于 Identity_Manager_3_5_1_Linux.iso 或 Identity_Manager_3_5_1_DVD.iso 上，而 AIX 和 Solaris 位于 Identity_Manager_3_5_1_Unix.iso 或 Identity_Manager_3_5_1_DVD.iso 上。

2 在主机上，请以 root 用户身份登录。

3 执行 安装目录中的 .bin 文件。

将当前工作目录更改为安装目录，即安装所在的位置。然后通过输入下列命令之一运行安装：

平台	示例路径	安装文件
Linux	linux/setup/	idm_linux.bin
Solaris	solaris/setup/	idm_solaris.bin
AIX	aix/setup/	idm_aix.bin

这些路径是安装映像根的相对路径，可能是展开此映像或装入 CD 的位置。

除非当前工作目录是安装程序所在的目录，否则安装程序将无法找到要安装的程序包。

4 选择运行安装程序要使用的语言，或使用默认语言 （英语）。键入一个编号，然后按 Enter 键。

```
 is 5174830 s in the future
tar: jre/lib/fonts/fallback/bsmi001p.ttf: time stamp 2007-01-29 17:20:20 is 5174
840 s in the future
tar: jre/lib/fonts/fallback: time stamp 2007-02-06 18:25:35 is 5869955 s in the
future
tar: jre/lib/fonts: time stamp 2007-02-06 18:25:51 is 5869971 s in the future
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...

Launching installer...

Preparing CONSOLE Mode Installation...

===============================================================================
Choose Locale...
----------------

    1- English
  ->2- 中文简体

CHOOSE LOCALE BY NUMBER:
```

5 查看欢迎信息，然后按 Enter 键继续安装。

6 按 Enter 键浏览许可证协议，如果同意这些使用条款，请输入 Y。如果不同意，请输入 N 退出安装程序。

7 指定编号 2 以安装已连接系统服务器。

安装集包含 Remote Loader 和以下驱动程序：Avaya、 Delimited Text、 Groupwise、JDBC、 JMS、 LDAP、 LINUX/Unix 设置、 Linux/UNIX Bidirectional、 Lotus Notes、PeopleSoft、 RACF、 Remedy、 SAP、 SIF、 Top Secret 和 Work Order。

```
安装集
    已连接系统服务器

产品组件：
    LDAP 驱动程序，
    SAP 驱动程序，
    JDBC 驱动程序，
    定界文本驱动程序，
    Lotus Notes 驱动程序，
    Remote Loader，
    Groupwise 驱动程序，
    Avaya 驱动程序，
    SOAP 驱动程序，
    Remedy 驱动程序，
    PeopleSoft 驱动程序，
    JMS 驱动程序，
    Linux/UNIX 双向驱动程序，
    Linux/UNIX 设置驱动程序，
    RACF 驱动程序，
    Top Secret 驱动程序


请按 <ENTER> 键继续：
```

8 查看 “预安装摘要”屏幕列出的项目。按 Enter 键安装组件。

```
===============================================================================
正在安装...
-------

 [==================|==================|==================|==================]
 [------------------|------------------|------------------|------------------]


===============================================================================
安装完成
----

恭喜。Novell Identity Manager 3.5 已经成功安装到您的系统中。

如果已经安装了 Identity Manager 插件，请重启动应用程序服务器。

按一下 <ENTER> 键退出安装程序：
```

默认情况下，将安装所有可用的驱动程序，这样，如果以后想要另一个驱动程序，就不需要运行安装程序。通过 iManager 或 Designer 配置驱动程序且将其部署之前，不使用这些驱动程序文件。

默认情况下， linux/unix 安装中不安装 identity Manager 驱动程序实用程序。要安装的话，必须手动将实用程序从 Identity Manager 安装 CD 复制到 Identity Manager 服务器。所有实用程序均位于*平台的*\setup\utilities 目录中。

9 当看到 “安装完成”屏幕时，按 Enter 键关闭安装程序。

4.9 Identity Manager 的非根安装

通过此 Identity Manager 发行版，您可以将 Identity Manager 元目录引擎安装到 eDirectory 的非根安装中。

必须先安装带最新增补程序的 Novell Security Services 2.0.4 (NMAS 3.1.3) 和非根 eDirectory 8.8，之后才能安装此选项。有关作为非根用户安装 NICI 的信息，请参见 Novell eDirectory 8.8 Installation Guide (http://www.novell.com/documentation/edir88/index.html) （《Novell

eDirectory 8.8 安装指南》）中的 “*3.0 Installing or Upgrading Novell eDirectory on Linux*”（3.0 在 Linux 上安装或升级 Novell eDirectory）标题下的 “*Installing NICI*”（安装 NICI）子部分。

安装 NICI 后，请遵循 Novell eDirectory 8.8 Installation Guide (http://www.novell.com/documentation/edir88/index.html) （《Novell eDirectory 8.8 安装指南》）中 “*3.0 Installing or Upgrading Novell eDirectory on Linux*”（3.0 在 Linux 上安装或升级 Novell eDirectory ）标题下的 “*Nonroot User Installing eDirectory 8.8* ”（非根用户安装 eDirectory 8.8）子部分中的非根 eDirectory 8.8 安装指导。

1 下载所需的 Identity Manager .iso 映像文件。可以从 Novell 下载站点下载 Identity Manager .iso (http://download.novell.com) 映像文件。

例如， Linux 位于 Identity_Manager_3_5_1_Linux.iso 或 Identity_Manager_3_5_1_DVD.iso 上，而 AIX 和 Solaris 位于 Identity_Manager_3_5_1_Unix.iso 或 Identity_Manager_3_5_1_DVD.iso 上。非根安装程序包括在 .iso 映像中。

2 在主计算机上，以对安装有非根 eDirectory 的目录具有写权限的用户身份登录。

3 执行 /setup/ 目录中的 idm-nonroot-install 文件。要执行该操作，请将当前工作目录更改为 setup 目录，然后输入以下命令运行非根安装：

./idm-nonroot-install

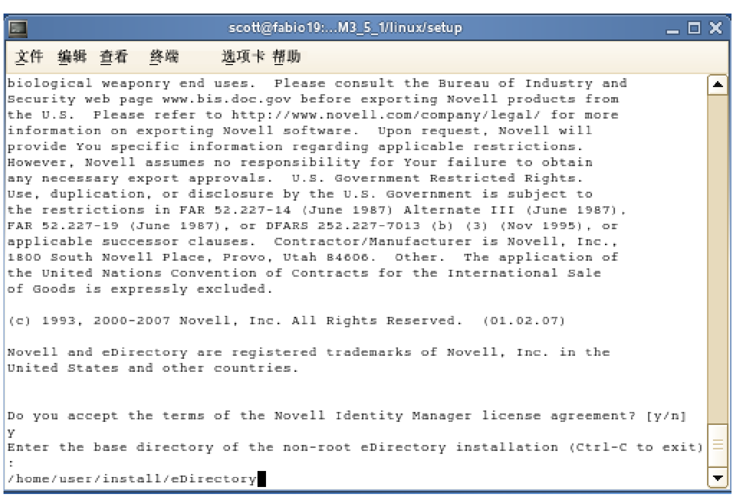
平台	示例路径	安装文件
Linux	linux/setup/	idm-nonroot-install
Solaris	solaris/setup/	idm-nonroot-install
AIX	aix/setup/	idm-nonroot-install

这些路径是相对于 iso 映像的相对路径，除非当前工作目录是安装程序所在的目录，否则安装程序将无法找到要安装的包。

4 按 Enter 键可显示最终用户许可证协议，然后按空格键可滚动整个协议。如果同意这些使用条款，请输入 Y。如果不同意，请输入 N 退出安装程序。

5 输入指向非根 eDirectory 驻留位置的路径。例如：

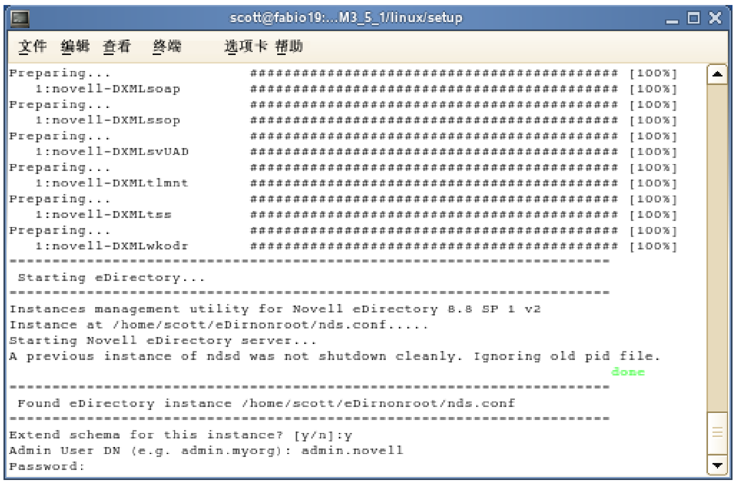
/home/user/installed/eDirectory



安装底稿将安装带有以下驱动程序的 Identity Manager：Avaya、 Delimited Text、GroupWise、JDBC、JMS、LDAP、Linux/UNIX 设置、Linux/UNIX Bidirectional、Lotus Notes、 PeopleSoft、 RACF、 Remedy、 SAP、 SIF、 Top Secret 和 Work Order。

6 然后，系统将要求您为已登录用户所有的每个 eDirectory 实例扩展纲要。对于每个实例，输入 Y 可扩展该实例的纲要，如果不想扩展该实例的纲要，则输入 N。

7 如果选择扩展纲要，请键入有权限扩展纲要的用户 （例如， admin.novell）的判别名 (DN)。选择具有足够权限扩展 eDirectory 纲要的用户 （对树的根具有主管权限的用户，比如 Admin）。



8 键入口令，然后按 Enter 键。需要对扩展的每个 eDirectory 实例执行步骤 7 和 8。

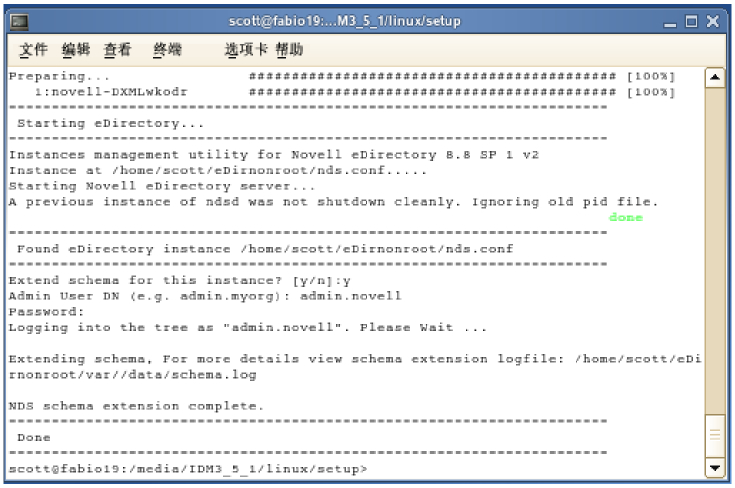
如果想要以后为其他 eDirectory 实例扩展纲要，请运行非根 eDirectory 安装 opt/novell/eDirectory/bin 子目录中的 idm-nonroot-install 底稿。以要扩展的 eDirectory 实例的拥有者身份登录后，运行该底稿。

安装底稿登录到 eDirectory 树，然后扩展纲要。如果要了解关于纲要扩展进程的更多信息，请转到 /home/user/eDirnonroot/var/data/schema.log 文件

默认情况下，将安装所有可用的驱动程序，这样，如果以后想要另一个驱动程序，就不需要运行安装程序。通过 iManager 或 Designer 配置驱动程序且将其部署之前，不使用这些驱动程序文件。

默认情况下， Linux/UNIX 安装中不安装 Identity Manager 驱动程序实用程序。要安装的话，必须手动将实用程序从 Identity Manager 安装 CD 复制到 Identity Manager 服务器。所有实用程序均位于*平台的*\setup\utilities 目录中。

9 完成纲要扩展过程中，会安装 Identity Manager。



4.10 安装后的任务

无需手动装载或卸装 Identity Manager，因为启动 Identity Manager 驱动程序启动时已装载 Identity Manager 模块。如果驱动程序的某个参数设置为 Autostart，并且驱动程序和 eDirectory 正在运行，则驱动程序将自动启动 Identity Manager 模块。如果驱动程序的某个参数设置为 “手动”，则启动 Identity Manager 驱动程序时将装载 Identity Manager 模块。

安装 Identity Manager 之后，需要配置安装的驱动程序，以实施根据业务过程定义的策略和要求。安装后的任务通常包括下列项目：

- 配置已连接系统。有关特定于驱动程序配置的指导，请参考 《Identity Manager 驱动程序文档 (http://www.novell.com/documentation/dirxmldrivers)》。
- 创建和配置驱动程序。使用 iManager 或 Designer 实用程序来创建驱动程序或配置现有驱动程序。请参见《*Designer 2.1 for Identity Manager 3.5.1* 指南》中的 “ 导入驱动程序配置文件 ”。
- 定义策略。使用 iManager 或 Designer 实用程序来定义驱动程序的策略，以满足您的业务需求。请参见 《*Designer 2.1 中的策略*》指南中的 “ 创建策略 ”，或参见 《*了解 Identity Manager 3.5.1* 指南》。
- 启动、停止或重新启动驱动程序。使用 iManager 或 Designer 实用程序来管理驱动程序的活动。请参见 《“Designer 2.1 for Identity Manager 3.5.1” 指南》中的 *导入驱动程序配置文件*。
- 激活 Identity Manager。请参见第 6 章 “激活 Novell Identity Manager 产品 ”（第 169 页）。

4.11 安装自定义驱动程序

自定义驱动程序可能包括下列项目：

- 一组 .jar 或 native （.dll、 .nlm, 或 .so）文件
- 用于配置驱动程序的 XML 规则文件
- 文档

有关创建或安装自定义驱动程序的更多信息，请参见 Novell 开发者工具 (http://developer.novell.com/ndk/dirxml-index.htm)。另请参见 《*Identity manager 3.5.1 管理指南*》中的 “编辑驱动程序文件”。

安装 User Application 5

本部分介绍如何安装 Identity Manager User Application。包括以下主题：

- 第 5.1 节 “安装的前提条件。”（第 93 页）
- 第 5.2 节 “安装和配置”（第 99 页）
- 第 5.3 节 “创建 User Application 驱动程序”（第 100 页）
- 第 5.4 节 “关于安装程序”（第 104 页）
- 第 5.5 节 “在 JBoss 应用程序服务器上从安装 GUI 安装 User Application”（第 105 页）
- 第 5.6 节 “在 WebSphere 应用程序服务器上安装 User Application”（第 132 页）
- 第 5.7 节 “从控制台界面安装 User Application”（第 158 页）
- 第 5.8 节 “使用单个命令安装 User Application”（第 158 页）
- 第 5.9 节 “安装后的任务”（第 163 页）
- 第 5.10 节 “安装后重新配置 IDM WAR 文件。”（第 167 页）
- 第 5.11 节 “查错”（第 167 页）

5.1 安装的前提条件。

在安装 Identity Manager User Application 之前，请校验是否满足以下要求：

表 5-1 *安装前提条件*

环境要求	说明
Java* Development Kit	下载并安装 Java 2 Platform Standard Edition Development Kit 5.0。使用 JRE V1.5.0_10。在 WebSphere 上，使用 IBM* JDK*，并应用无限制的策略文件。 将 JAVA_HOME 环境变量设置为指向 JDK，以配合 User Application 使用。或者，在 User Application 安装过程中手动指定路径，以覆盖 JAVA_HOME。 ◆ 在 Linux 或 Solaris 命令提示符下，输入 echo $JAVA_HOME。要创建或更改 JAVA_HOME，请创建或编辑 ~/.profile （在 SUSE® Linux 中）： # Java Home export JAVA_HOME=/usr/java/jdk1.5.0_10 #JRE HOME export JRE_HOME=$JAVA_HOME/jre ◆ 在 Windows 中，查看*控制面板* > *系统* > *高级* > *环境变量* > *系统变量*。

环境要求	说明
JBoss 应用程序服务器	如果使用 JBoss，请下载并安装 JBoss 4.2.0 应用程序服务器 .（安装 User Application 之后启动服务器。参见第 5.9 节 “安装后的任务” （第 163 页））。 **RAM：**运行 User Application 时，建议用于 JBoss 应用程序服务器的 RAM 至少为 512 MB。 **端口：**将应用程序服务器所使用的端口记录下来。（应用程序服务器的默认端口为 8080。） **SSL：**如果计划使用外部口令管理，请在部署 User Application 和 IDMPwdMgt.war 文件的 JBoss 服务器上启用 SSL。有关指导，请参见 JBoss 文档。还需要确保在防火墙上打开 SSL 端口。有关 IDMPwdMgt.war 文件的更多信息，请参见第 5.9.4 节 “访问外部口令 WAR” （第 164 页）以及 《*IDM 3.5.1 User Application：管理指南* (http://www.novell.com/documentation/idm35/index.html)》。
WebSphere 应用程序服务器	如果使用 WebSphere，请下载并安装 WebSphere 6.1 应用程序服务器。
启用 iChain 注销	通过在 Novell Access Manager™ 或 iChain® 中启用 “Cookie 转发” 选项，可以在 Identity Manager User Application 中启用 ICS 注销。
数据库	安装数据库和数据库驱动程序，并创建数据库或数据库实例。记下主机和端口，这将在第 5.5.7 节 “指定数据库主机和端口” （第 114 页）中用到。记下数据库名称、用户名和用户口令，这将在第 5.5.8 节 “指定数据库名称和特权用户” （第 115 页）中用到。 数据源文件必须指向数据库。此处理方式根据您的应用程序服务器而异。对于 JBoss， User Application 安装程序将创建一个指向此数据库的应用程序服务器数据源文件，并根据 User Application WAR 文件命名此文件。对于 WebSphere，请在安装前手动配置数据源。 数据库必须启用了 UTF-8。 是要通过 IDM User Application 实用程序安装 MySQL，还是自行安装 MySQL，请阅读第 5.1.3 节 “配置 MySQL 数据库” （第 98 页）。 **注释：**如果计划迁移数据库，在安装程序中选择迁移选项之前，请启动该数据库。如果不迁移数据库，则安装 User Application 过程中无需运行数据库。记住在启动应用程序服务器之前启动数据库。
如果在 LINUX 或 Solaris 上安装 IDM 3.5.1 User Application	默认安装位置为 /opt/novell/idm。可以在安装过程中选择其他默认安装目录。请确保存在此目录，并且非根用户对此目录有写权限。
如果在 Windows 上安装 IDM 3.5.1 User Application	**安装目录：**默认安装位置为 C:\Novell\IDM。要确保存在此目录，并且可写。可以在安装过程中选择其他默认安装目录。
Identity Manager 3.5.1	必须首先安装 Identity Manager 3.5.1 元目录服务器，之后才能创建 User Application 驱动程序和安装 User Application。
User Application 驱动程序	在安装 User Application 之前，必须已经存在 User Application 驱动程序 （但没有启用）。
身份库 访问	User Application 需要用户对将驻留有 User Application 用户的环境具有管理员访问权限。
IDM User Application 储存器	安装 User Application 的计算机必须具有 320 MB 以上的可用储存空间。

确保满足所有前提条件之后，请按照以下部分给出的安装指导进行操作：

- 第 5.1.1 节 “安装 JBoss 应用程序服务器和 MySQL 数据库”（第 95 页）
- 第 5.1.2 节 “安装 JBoss 应用程序服务器作为一项服务”（第 97 页）
- 第 5.1.3 节 “配置 MySQL 数据库”（第 98 页）

5.1.1 安装 JBoss 应用程序服务器和 MySQL 数据库

使用 Jbossmysql 实用程序在系统中安装 JBoss 应用程序服务器和 MySQL。

此实用程序并不安装 JBoss 应用程序服务作为 Windows 服务。要将 JBoss 应用程序服务器作为 Windows 系统上的一个服务来安装，请参见第 5.1.2 节 “安装 JBoss 应用程序服务器作为一项服务”（第 97 页）。

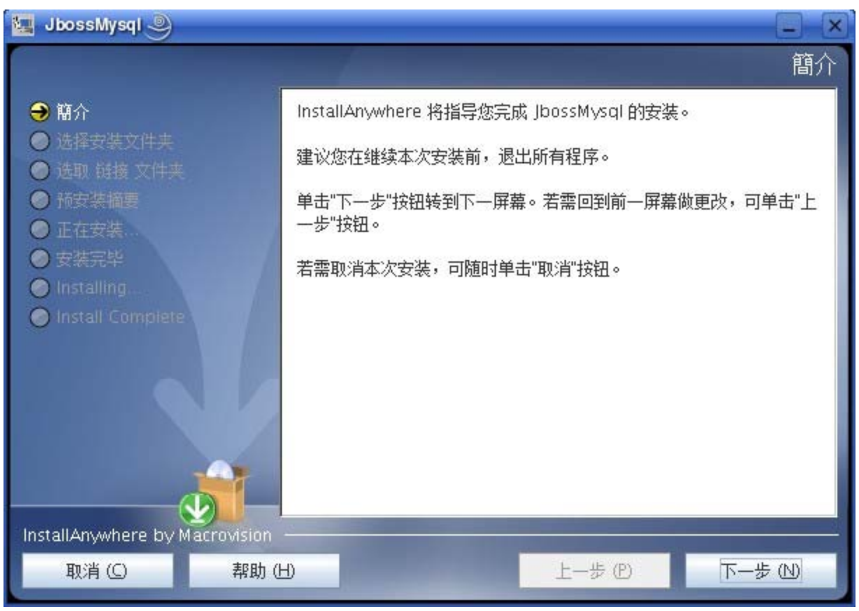
1 找到并执行 JbossMysql.bin 或 JbossMysql.exe。可在以下位置找到绑定在 User Application 上的此实用程序：

   /linux/user_application （对于 Linux）
   /nt/user_application （对于 Windows）

   Solaris 不提供此实用程序。

2 选择区域设置。

3 阅读介绍页面，然后单击 *下一步*。



4 选择要安装的产品，然后单击*下一步*。

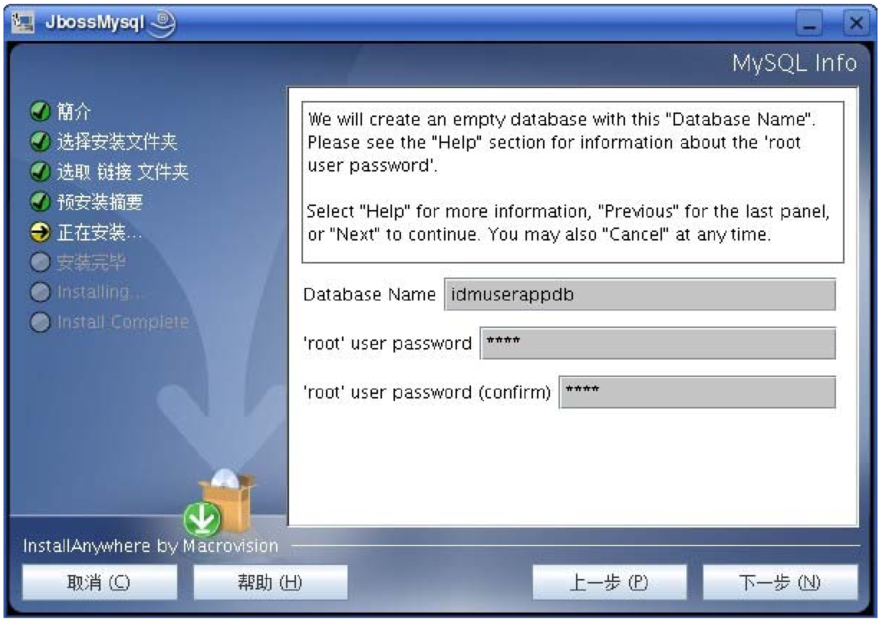


5 单击*选择*以选择要安装选定产品的根文件夹，然后单击*下一步*。



6 指定数据库的名称。User Application 安装需要此名称。

7 指定数据库 root 用户口令。



8 单击*下一步*。

9 在 “安装前摘要”中检查指定的设置，然后单击*安装*。



安装选定产品之后，实用程序将显示一条成功完成安装的讯息。如果安装了 MySQL 数据库，请继续第 5.1.3 节 “配置 MySQL 数据库”（第 98 页）。

5.1.2 安装 JBoss 应用程序服务器作为一项服务

要作为一项服务运行 JBoss 应用程序服务器，请使用 Java Service Wrapper 或第三方实用程序。请访问 http://wiki.jboss.org/wiki/Wiki.jsp?page=RunJBossAsAServiceOnWindows

(http://wiki.jboss.org/wiki/Wiki.jsp?page=RunJBossAsAServiceOnWindows)，了解 JBoss 的指导。

- 使用 Java Service Wrapper （第 98 页）
- 使用第三方实用程序 （第 98 页）

使用 Java Service Wrapper

通过 Java Service Wrapper，可以安装、启动和停止 JBoss 应用程序服务器作为 Windows 服务或 Linux 或 UNIX 守护进程。请在因特网上查找可用的实用程序和下载站点。

此类封装程序中的一个位于 http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html (http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html)：通过 JMX 管理此封装程序 （请参见 http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss (http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss)）。某些示例配置文件包括：

wrapper.conf :

wrapper.java.command=%JAVA_HOME%/bin/java

wrapper.java.mainclass=org.tanukisoftware.wrapper.WrapperSimpleApp

wrapper.java.classpath.1=%JBOSS_HOME%/server/default/lib/wrapper.jar

wrapper.java.classpath.2=%JAVA_HOME%/lib/tools.jar wrapper.java.classpath.3=./run.jar

wrapper.java.library.path.1=%JBOSS_HOME%/server/default/lib wrapper.java.additional.1=-server wrapper.app.parameter.1=org.jboss.Main wrapper.logfile=%JBOSS_HOME%/server/default/log/wrapper.log wrapper.ntservice.name=JBoss wrapper.ntservice.displayname=JBoss Server

---

警告：必须正确设置 JBOSS_HOME 环境变量。封装程序本身不设置此变量。

---

java-service-wrapper-service.xml : <Xxml version="1.0" encoding="UTF-8"?><!DOCTYPE server><server> <mbean code="org.tanukisoftware.wrapper.jmx.WrapperManager" name="JavaServiceWrapper:service=WrapperManager"/> <mbean code="org.tanukisoftware.wrapper.jmx.WrapperManagerTesting" name="JavaServiceWrapper:service=WrapperManagerTesting"/></server

使用第三方实用程序

对于先前版本，可以使用第三方实用程序 （如 JavaService）作为一项 Windows 服务安装、启动和停止 JBoss 应用程序服务器。

警告：JBoss 不再建议使用 JavaService。有关详细信息，请参见 http://wiki.jboss.org/wiki/Wiki.jsp?page=JavaService (http://wiki.jboss.org/wiki/Wiki.jsp?page=JavaService)。

5.1.3 配置 MySQL 数据库

必须设置 MySQL 配置，以使 MySQL 和 Identity manager 3.5.1 能够配合工作。如果自己安装 MySQL，必须自行设置。如果通过使用 JbossMysql 实用程序安装 MySQL，则实用程序将为您设置正确的值，但需要知道为以下项目保留的值：

- 字符集 （第 99 页）
- INNODB 存储引擎和表类型 （第 99 页）

- 区分大小写 （第 99 页）

字符集

将整个服务器或仅仅某个数据库的字符集指定为 UTF-8。要在整个服务器范围内指定 UTF-8，可在 My.cnf （Linux 或 Solaris）或 My.ini (Windows) 中加入以下选项：

character-set-server=utf8 或

要在创建数据库时为该数据库指定该字符集，请使用以下命令：

create database databasename character set utf8 collate utf8_bin;

如果为数据库设置该字符集，还必须在 IDM-ds.xml 文件的 JDBC URL 中指定该字符集，如：

<connection-url>jdbc:mysql://localhost:3306/
databasename?useUnicode=true&characterEncoding

INNODB 存储引擎和表类型

User Application 使用了 INNODB 存储引擎，通过它可以选择为 MySQL 指定 INNODB 表类型。如果创建 MySQL 表时没有指定表类型，默认情况下，该表采用 MyISAM 表类型。如果选择在 Identity Manager 安装过程中安装 MySQL，则在此过程中安装的 MySQL 采用指定的 INNODB 表类型。为确保 MySQL 服务器使用 INNODB，请校验 my.cnf （Linux 或 Solaris）或 my.ini (Windows) 中包含以下选项：

default-table-type=innodb

它不应包含 skip-innodb 选项。

区分大小写

如果计划跨服务器或平台备份或恢复数据，请确保所有服务器或平台上的大小写保持一致。要确保该一致性，请为所有 my.cnf （Linux 或 Solaris）或 my.ini (Windows) 文件中的 lower_case_table_names 指定相同的值 （0 或 1），而不是接受默认值 （Windows 默认为 0，而 Linux 默认为 1。）请在创建数据库保存 Identity Manager 表之前指定该值。例如，对于所有计划备份和恢复数据库的平台，可以指定

lower_case_table_names=1

（在 my.cnf 和 my.ini 文件中）。

5.2 安装和配置

1 创建 User Application 驱动程序并保留为关闭。

   此步骤在身份库 中创建新的对象。一部分对象将采用默认数据值。有关更多信息，请参见第 5.3 节 “创建 User Application 驱动程序”（第 100 页）。

2 运行 User Application 的安装程序。

   有关更多信息，请参见第 5.6 节 “在 WebSphere 应用程序服务器上安装 User Application”（第 132 页）或第 5.5 节 “在 JBoss 应用程序服务器上从安装 GUI 安装 User Application”（第 105 页）。

   WebSphere 用户必须手动部署 WAR 文件。

重要：对于安装 Identity Manager User Application，在安装之前，要求已经存在 User Application 驱动程序。但是，必须在安装 Identity Manager User Application *之后*启动驱动程序，否则 User Application 驱动程序可能会返回错误。

5.3 创建 User Application 驱动程序

必须为每个 User Application 创建单独的 User Application 驱动程序，群集中的 User Application 除外。同一群集中的 User Application 必须共享一个 User Application 驱动程序。有关运行群集中的 User Application 的信息，请参见《*Identity Manager 3.5.1 User Application 管理指南* (http://www.novell.com/documentation/idm35/index.html)》。

User Application 在驱动程序中存储特定于应用程序的数据，以控制和配置应用程序的环境。这包括应用程序服务器群集信息和工作流程引擎配置。

重要：如果配置一组非群集 User Application 以共享单个驱动程序，将导致运行于 User Application 内的一个或多个组件出现不确定和错误配置的现象。所导致的问题的来源难以检测。

要创建 User Application 驱动程序并将其与驱动程序集关联，请执行下列操作：

1 登录身份库 with iManager（如果尚未登录的话）。

2 转至*角色和任务 > Identity Manager 实用程序*，然后选择*新建驱动程序*起动“创建驱动程序”向导。

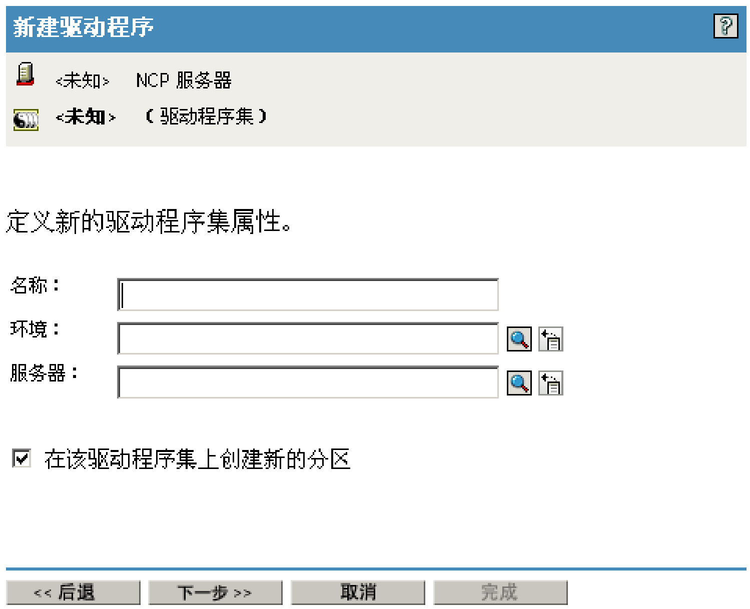


3 要在现有驱动程序集中创建驱动程序，选中*在现有驱动程序中*，单击对象选择器图表，选择驱动程序集对象，单击*下一步*，然后继续步骤 4。

或

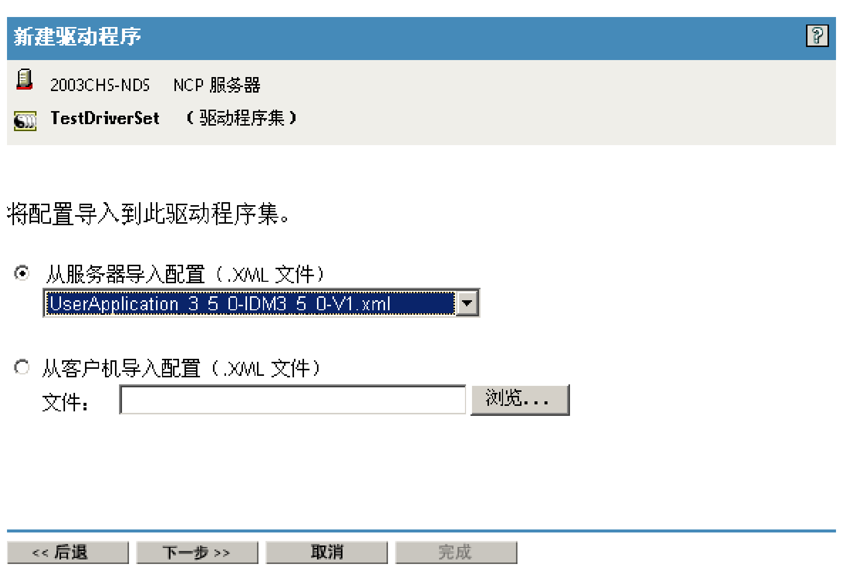
如果需要新建驱动程序集（比如，如果要将 User Application 驱动程序放置到不同于其他驱动程序的服务器上），选择*在新驱动程序集中*，单击*下一步*，然后定义新驱动程序集的属性。

3a 指定新驱动程序集的名称、环境和服务器。



3b 单击*下一步*。

4 单击*从服务器导入驱动程序配置（.XML 文件）*。



5 从下拉列表中选择 *UserApplication.xml*。

这便是新驱动程序的配置文件。

6 单击 *下一步*。

如果此下拉列表中未列出 *UserApplication.xml*，则可能是没有运行 Identity Manager 3.5.1 安装的基于万维网的管理服务器部分。

7 将提示您提供驱动程序的参数。（通过滚动查看全部内容。）将参数记录下来，在安装 User Application 时将用到它们。

字段	说明
驱动程序名	创建的驱动程序的名称。
鉴定 ID	User Application 管理员的判别名。这是将赋予其管理 User Application 入口权限的 User Application 管理员。使用 eDirectory™ 格式，例如 admin.orgunit.novell，或通过浏览查找用户。这是一个必需的字段。
口令	鉴定 ID 中所指定 User Application 管理员的口令。
应用程序环境	User Application 环境。此为 User Application WAR 文件的 URL 的环境部分。默认值为：IDM
主机	部署 Identity Manager User Application 的应用程序服务器的主机名或 IP 地址。 如果该应用程序服务器运行于群集中，请键入发送程序的主机名或 IP 地址。
端口	以上所列主机的端口。
允许覆盖启动程序： （值为 “否” / “是”）	通过选择*是*，允许供应管理员以被指定为代理的用户的名义启动工作流程。

8 单击 *下一步*。

9 单击*定义安全性等效*以打开 “安全性等效”窗口 。浏览并选择管理员或其他主管对象，然后单击*添加*。

此步骤可为驱动程序指定所需的安全性许可权限。可以在 Identity Manager 文档中找到有关此步骤的重要性的细节。

10 （可选，但不推荐）单击*排除管理角色*。

11 单击*添加*，然后选择要排除驱动程序操作的用户 （比如管理角色）。

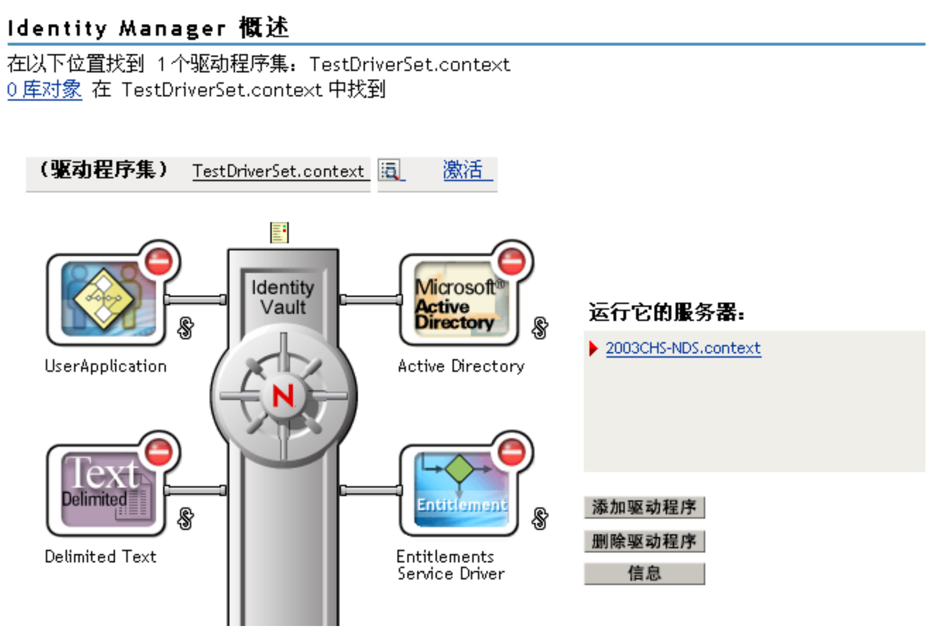
12 单击两次*确定*，然后单击 *下一步*。

13 单击*确定*关闭“安全性等效”窗口并显示摘要页。



14 如果信息准确无误，单击*完成*或*浏览完毕*。

重要：默认情况下，驱动程序为关闭状态。将驱动程序保持为关闭状态，直到已安装 User Application。



5.4 关于安装程序

User Application 安装程序执行以下操作：

- 指定要使用的现有应用程序服务器版本。
- 指定要使用的现有数据库版本，例如 MYSQL、 Oracle 或 Microsoft SQL Server。该数据库存储 User Application 数据和 User Application 配置信息。
- 配置 JDK 证书文件，以便 User Application （运行于应用程序服务器上）能够安全地与身份库和 User Application 驱动程序通讯。
- 配置 Novell Identity Manager User Application 的 Java 万维网应用程序存档 (WAR) 文件，并将其部署到 JBoss 应用程序服务器。
- 根据需要启用 Novell Audit 日志记录。
- 允许导入现有主密钥，以恢复特定 User Application 安装和支持群集。

- 第 5.4.1 节 “安装底稿和可执行文件”（第 104 页）
- 第 5.4.2 节 “安装时要求的值”（第 105 页）

可以以下三种模式之一运行安装程序：

- 图形用户界面。参见 第 5.5 节 “在 JBoss 应用程序服务器上从安装 GUI 安装 User Application”（第 105 页）
- 控制台 （命令行）界面。参见 第 5.7 节 “从控制台界面安装 User Application”（第 158 页）
- 静默安装。请参见第 5.8 节 “使用单个命令安装 User Application”（第 158 页）。

5.4.1 安装底稿和可执行文件

通过以下方式之一获取 Identity Manager 3.5.1 安装文件：

- 向系统中下载正确的 User Application .iso 映像或 .zip 文件：Identity_Manager_3_5_1_User_Application.iso 或 Identity_Manager_3_5_1_User_Application_Provisioning.iso。可以从 Novell 下载 (http://download.novell.com/index.jsp) 下载。
- 从 Novell, Inc. 下载产品 DVD Identity_Manager_3_5_1_DVD.iso。

表 5-2 列出了安装 Identity Manager 3.5.1 User Application 所需的文件和底稿。

表 5-2 *安装 Identity Manager 3.5.1 User Application 所需的文件和底稿*

文件	说明
User Application WAR	选择其中一个： **IDM.war**。包括具有身份自助服务功能的 Identity Manager 3.5.1 User Application。 **IDMProv.war**。包含带 Identity 自助服务功能和供应模块的 Identity manager 3.5.1 User Application。

系统的 WAR 文件以及 IdmUserApp.jar 和 silent.properties 文件初始位于以下与系统相关的递送 CD 目录中：

/linux/user_application （对于 Linux）
/nt/user_application （对于 Windows）
/solaris/user_application （对于 Solaris）

5.4.2 安装时要求的值

表 5-3 为记录计划安装 JBoss 时使用的安装参数的工作表。也可以在安装时设置 User Application 配置参数，请参见第 5.5.14 节 “配置 User Application”（第 121 页）。

***表 5-3** 安装参数工作表对于 JBoss：*

参数	样本值	指定的值
安装文件夹	C:\IDM\IDMinstalllocation	
数据库平台	MySQL	
数据库主机	localhost	
数据库端口	3306	
数据库名称或 SID	IDM	
数据库用户	root	
数据库用户口令		
Java 根文件夹	C:\Java\jdk1.5.0_10\	
(JBoss) 根文件夹	C:\jboss	
JBoss 主机	localhost	
JBoss 端口	8080	
工作流程引擎 ID （对于群集安装。对于每个群集号必须唯一。）		
应用程序名称 （URL 环境）	IDM	
Novell Audit 服务器	[名称或 IP 地址]	
经过加密的主密钥。请参见第 5.5.13 节 “指定主密钥”（第 119 页）。	_+FEJEefMAglH0A==:3VRmp04lub21Y3GpdaXCY)LGqS1nBaL/	

5.5 在 JBoss 应用程序服务器上从安装 GUI 安装 User Application

本部分说明如何在 JBoss 应用程序服务器上通过使用安装程序的图形用户界面版本安装 Identity Manager User Application。

- 第 5.5.1 节 “运行安装程序 GUI”（第 106 页）

- 第 5.5.2 节 “选择应用程序服务器平台”（第 108 页）
- 第 5.5.3 节 “迁移数据库”（第 108 页）
- 第 5.5.4 节 “指定 WAR 的位置”（第 110 页）
- 第 5.5.5 节 “选择安装文件夹”（第 110 页）
- 第 5.5.6 节 “选择数据库平台”（第 112 页）
- 第 5.5.7 节 “指定数据库主机和端口”（第 114 页）
- 第 5.5.8 节 “指定数据库名称和特权用户”（第 115 页）
- 第 5.5.9 节 “指定 Java 根目录”（第 116 页）
- 第 5.5.10 节 “指定 JBoss 应用程序服务器设置”（第 116 页）
- 第 5.5.11 节 “选择应用程序服务器配置类型”（第 118 页）
- 第 5.5.12 节 “启用 Novell Audit 日志记录”（第 119 页）
- 第 5.5.13 节 “指定主密钥”（第 119 页）
- 第 5.5.14 节 “配置 User Application”（第 121 页）
- 第 5.5.15 节 “校验选择并安装”（第 132 页）
- 第 5.5.16 节 “查看日志文件”（第 132 页）

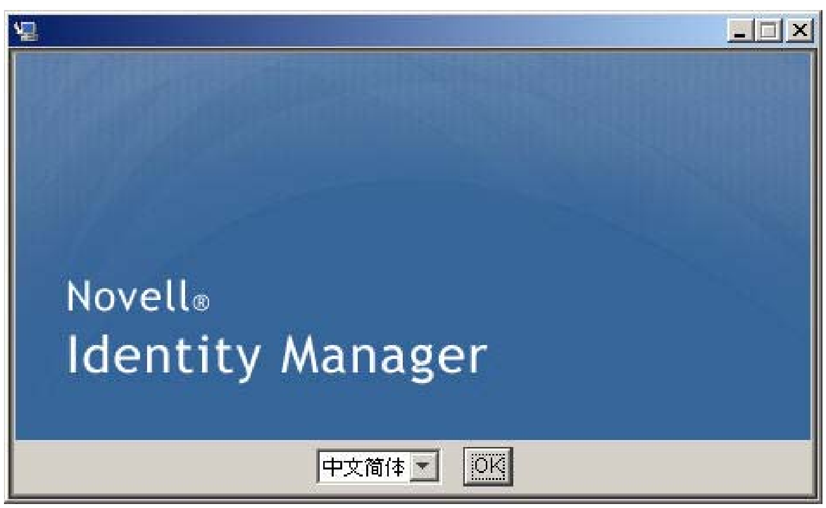
5.5.1 运行安装程序 GUI

1 浏览找到包含安装文件的目录，如表 5-2 （第 104 页）中所述。

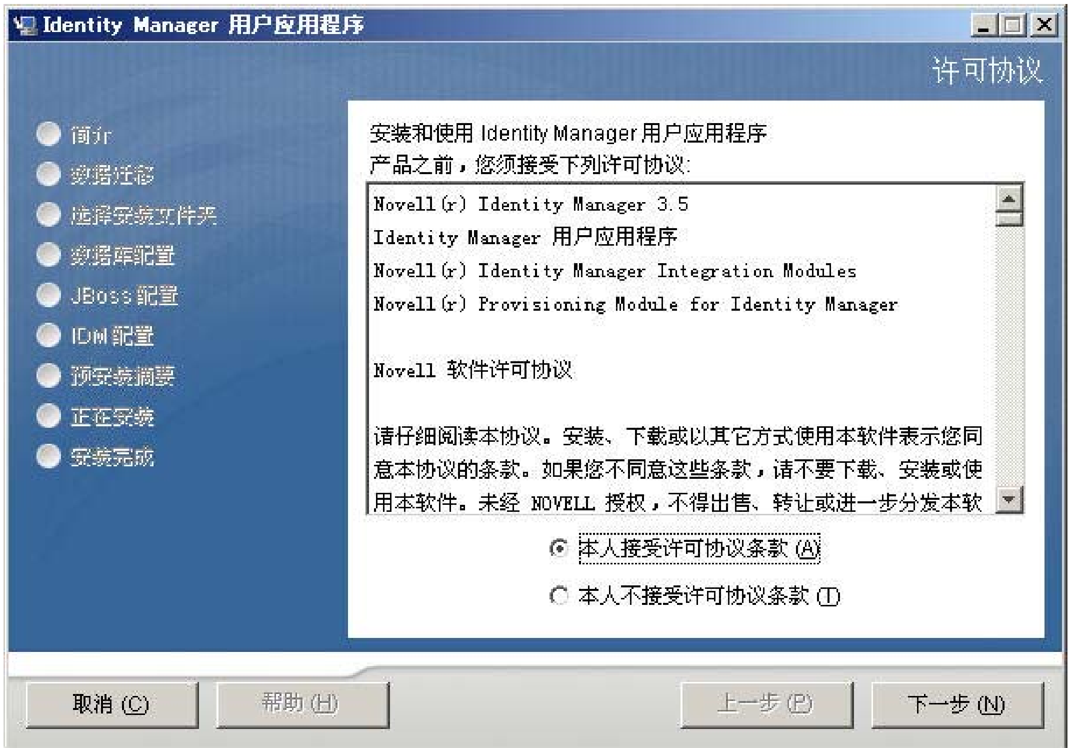
2 从命令行起动平台的安装程序：

```
java -jar IdmUserApp.jar
```

3 从下拉菜单中选择一种语言，然后单击*确定*。



4 阅读许可证协议，单击*我接受许可证协议中的条款*，然后单击*下一步*。

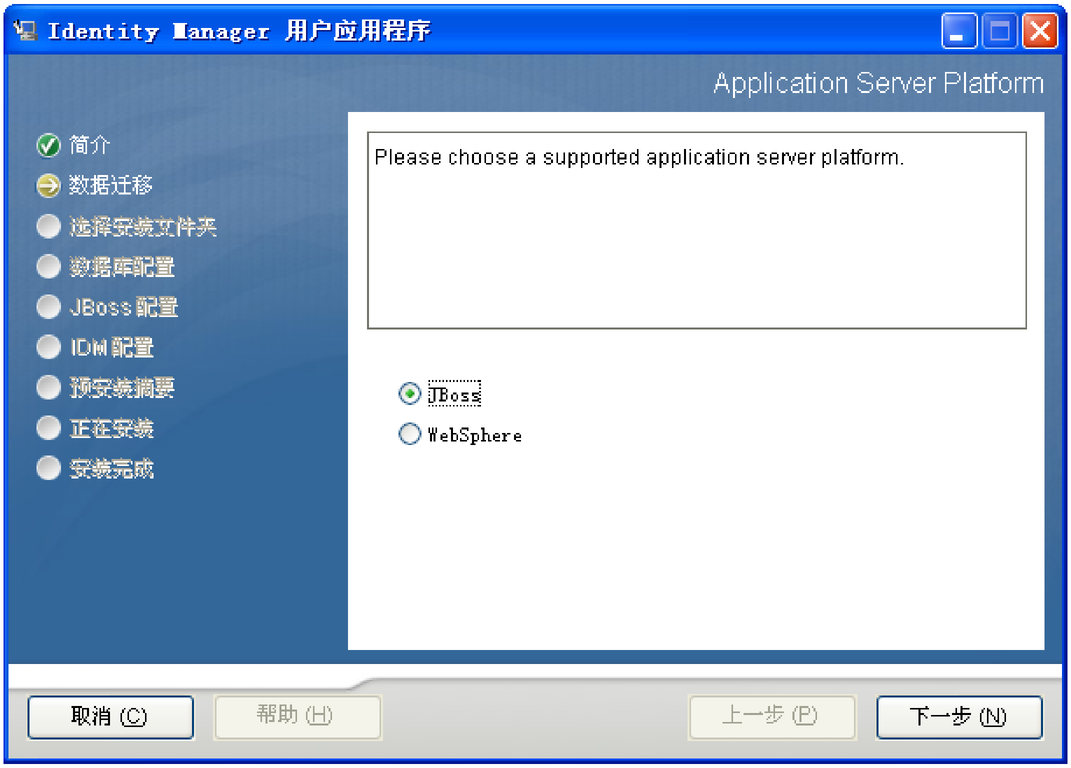


5 阅读安装向导的“介绍”页，然后单击*下一步*。

6 继续第 5.5.2 节 “选择应用程序服务器平台”（第 108 页）。

5.5.2 选择应用程序服务器平台

1 选择 JBoss 应用程序服务器平台，然后单击*下一步*。



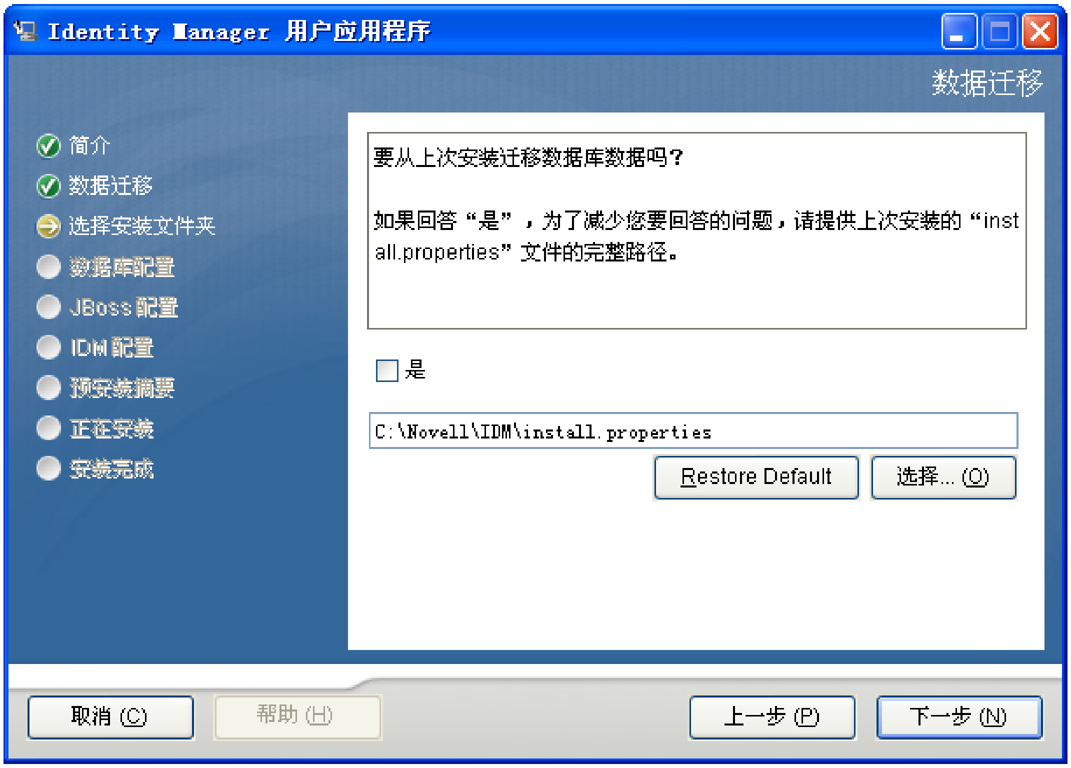
5.5.3 迁移数据库

如果不想迁移数据库，请单击*下一步*，然后继续第 5.5.4 节 "指定 WAR 的位置" （第 110 页）。

如果要使用来自版本 3.0 或版本 3.01 User Application 的现有数据库，则必须进行数据库的迁移。

1 校验已启动了要迁移的数据库。
2 单击安装程序的 "数据迁移" 页中的*是*。
3 单击*选择*浏览 Identity Manager 3.0 或 3.01 User Application 安装目录中的 install.properties 文件。

通过指定以前安装的 install.properties 文件的位置，可以减少必须在下面页面中指定的项目的数目。



4 系统要求您确认数据库类型、主机名和端口。确认这些内容后，单击 *下一步*。



5 单击*下一步*继续到第 5.5.4 节 “指定 WAR 的位置”（第 110 页）或第 5.5.5 节 “选择安装文件夹”（第 110 页）。

User Application 安装程序更新 User Application，并将 V3.0 或 3.0.1 数据库中的数据迁移到 V3.5.1 所使用的数据库。有迁移数据库的信息及其其他步骤，请参见 《*Identity Manager User Application：迁移指南* (http://www.novell.com/documentation/idm35/index.html)》。

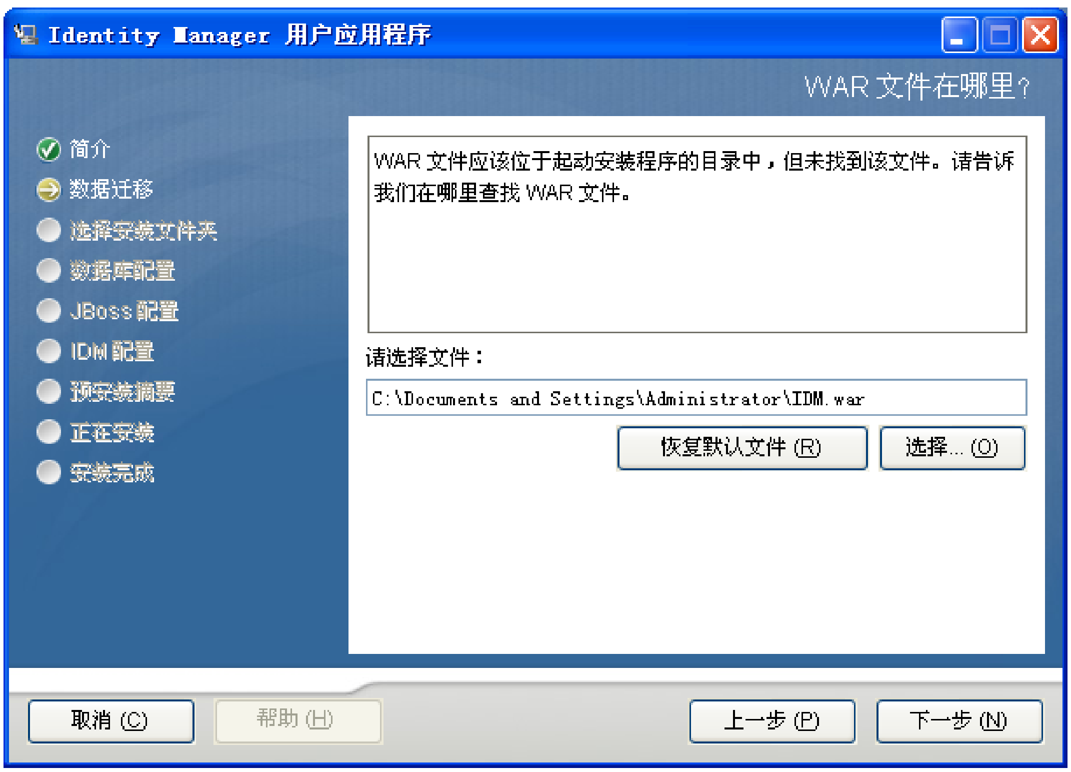
5.5.4 指定 WAR 的位置

如果 Identity Manager User Application WAR 文件所在的目录不同于安装程序，安装程序将提示提供 WAR 的路径。

1 如果 WAR 在默认位置，请单击*恢复默认文件夹*。

或者，要指定 WAR 文件的位置，单击*选择*并选择某个位置。

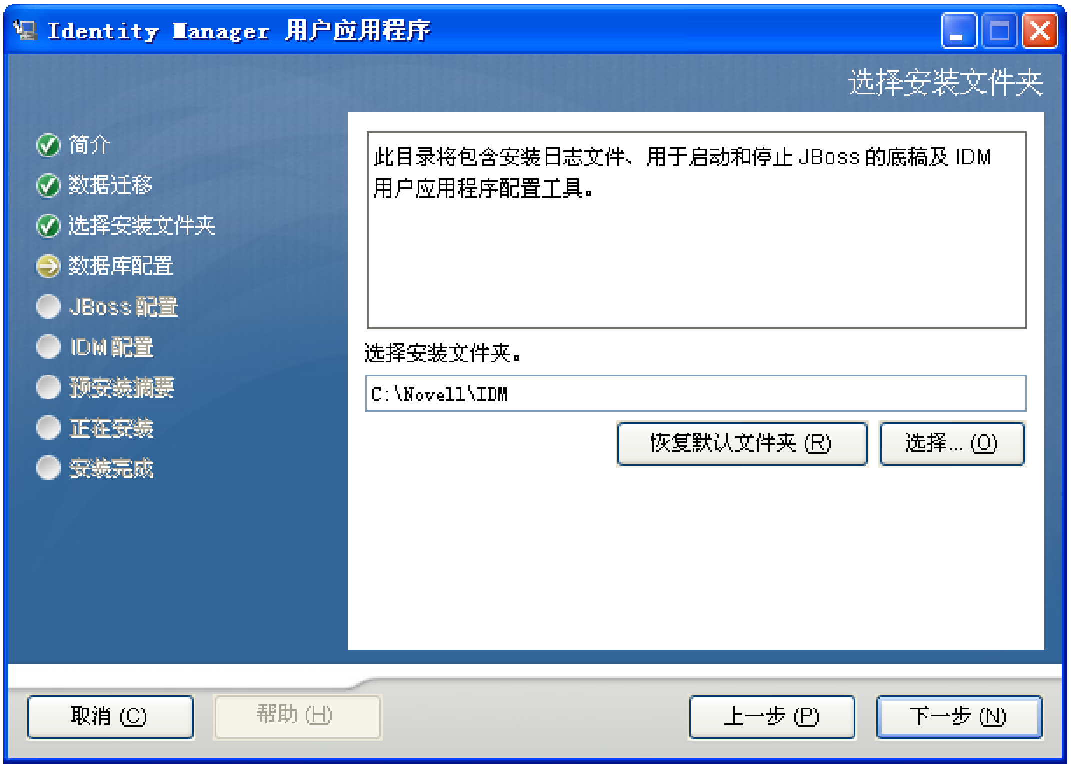
2 单击*下一步*，然后继续第 5.5.5 节 “选择安装文件夹”（第 110 页）。



5.5.5 选择安装文件夹

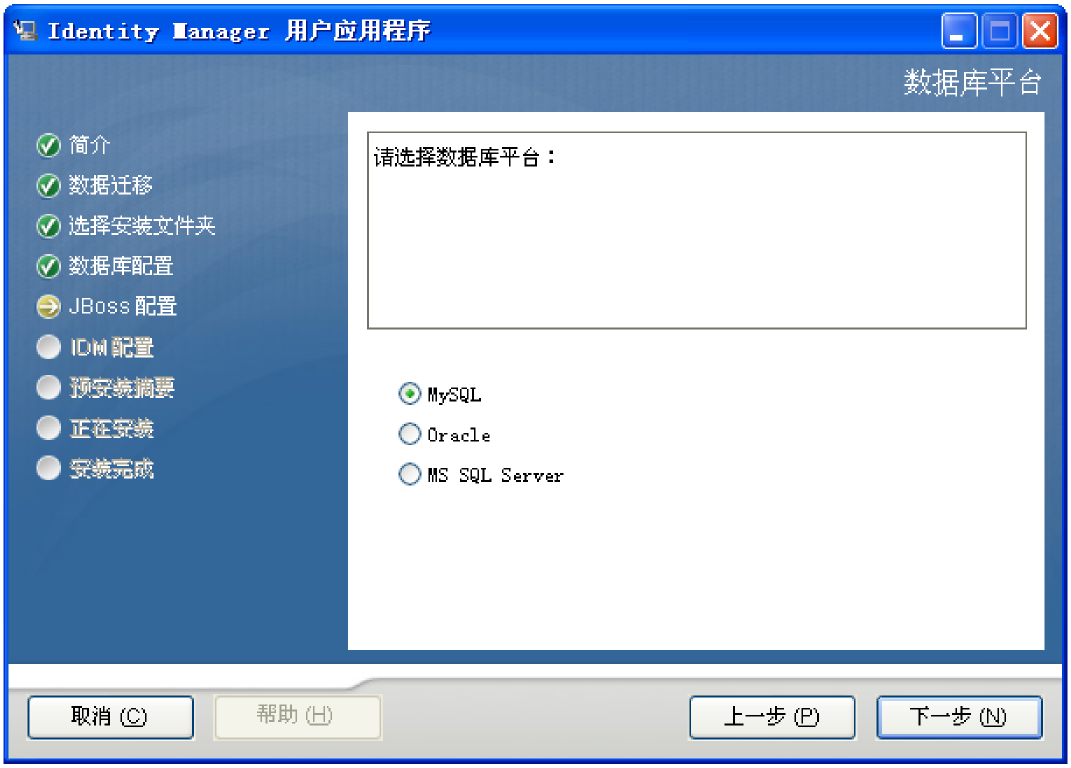
1 在 “选择安装文件夹”页，选择安装 User Application 的位置。如果要记住和使用默认位置，单击*恢复默认文件夹*；如果要为安装文件选择其他位置，单击*选择*并浏览某个位置。

2 单击 *下一步*，然后继续第 5.5.6 节 “选择数据库平台”（第 112 页）。



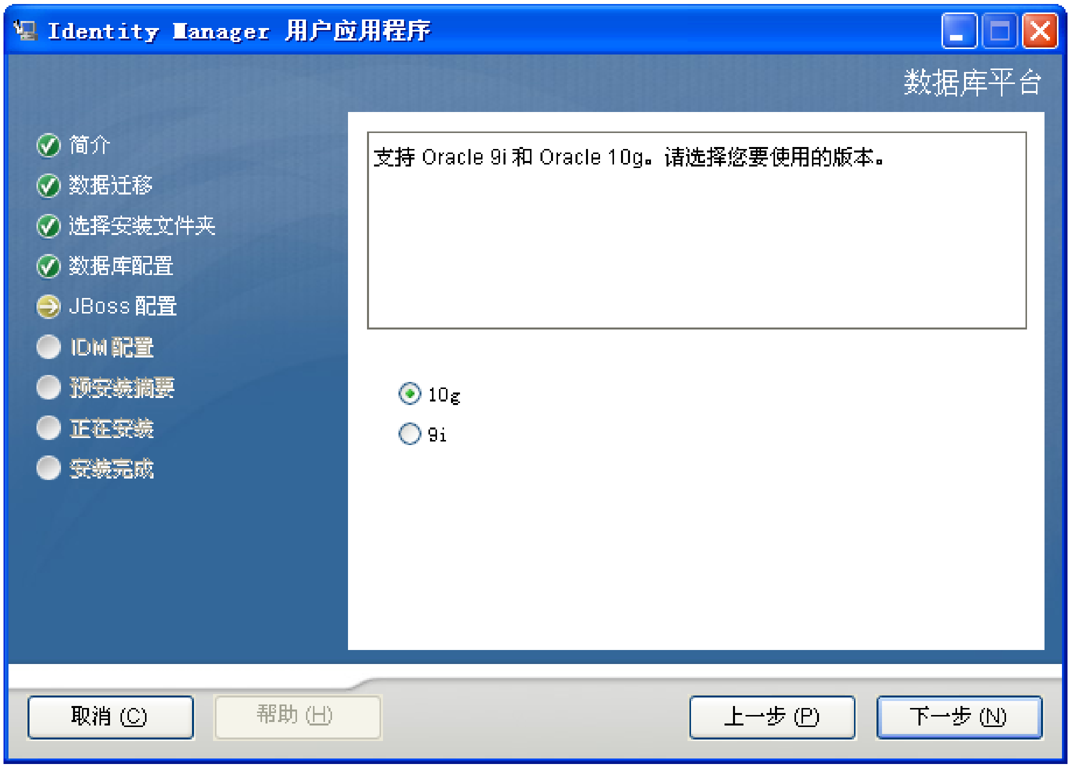
5.5.6 选择数据库平台

1 选择要使用的数据库平台。



2 如果使用的是 Oracle 数据库，请继续步骤 3。否则，请跳至步骤 4。

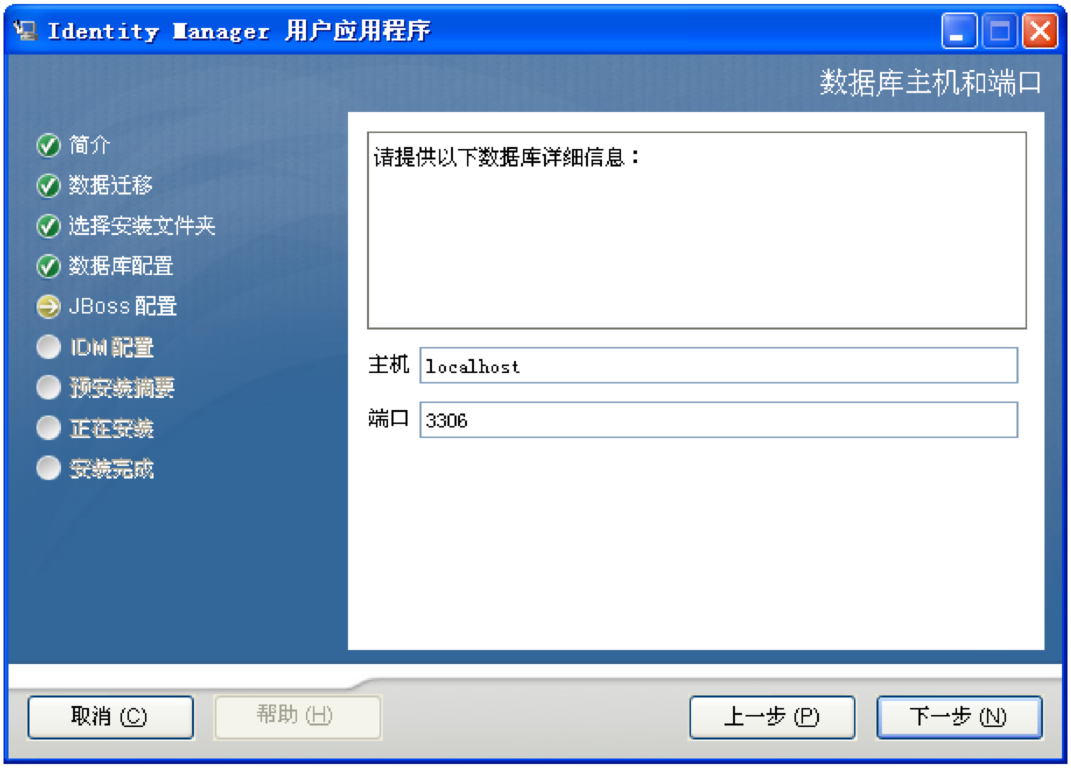
3 如果使用的是 Oracle 数据库，安装程序将询问所使用的版本。选择使用的版本。



4 单击 *下一步*，然后继续第 5.5.7 节 “指定数据库主机和端口”（第 114 页）。

5.5.7 指定数据库主机和端口

1 填写以下字段：

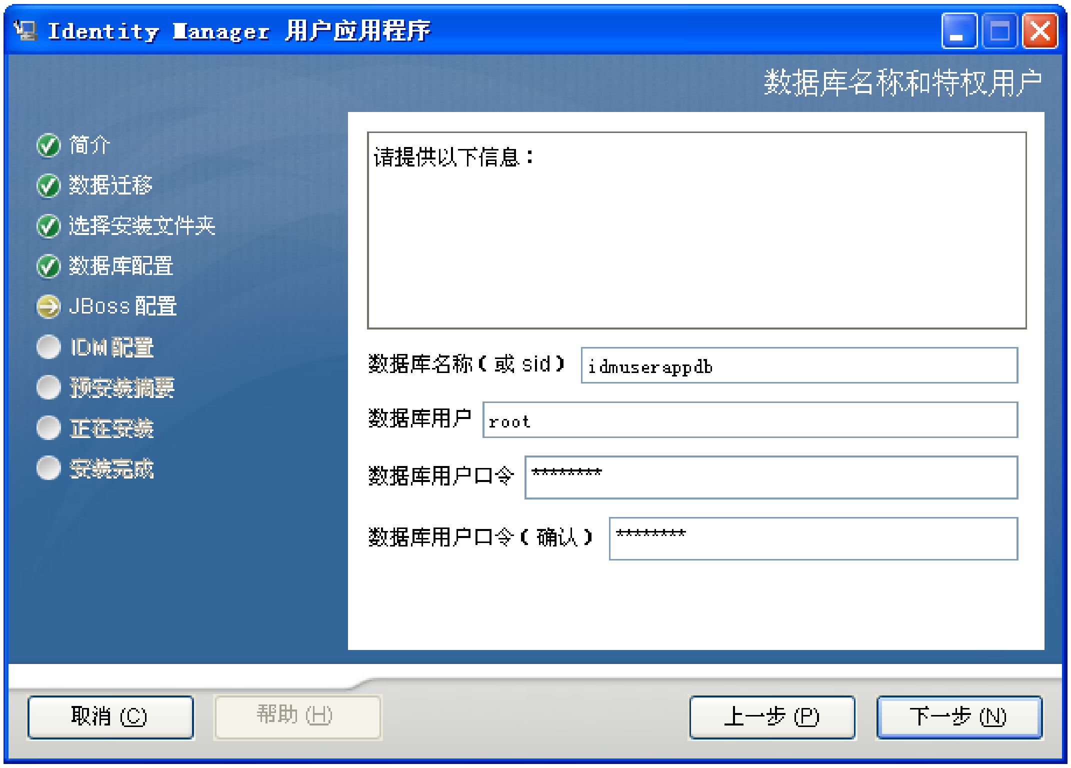


字段	说明
主机	指定数据库服务器的主机名或 IP 地址。
	对于群集，对其中每个成员指定相同的主机名或 IP 地址。
端口	指定数据库的侦听器端口号。
	对于群集，对其中每个成员指定相同的端口。

2 单击 *下一步*，然后继续第 5.5.8 节 “指定数据库名称和特权用户”（第 115 页）。

5.5.8 指定数据库名称和特权用户

1 填写以下字段：

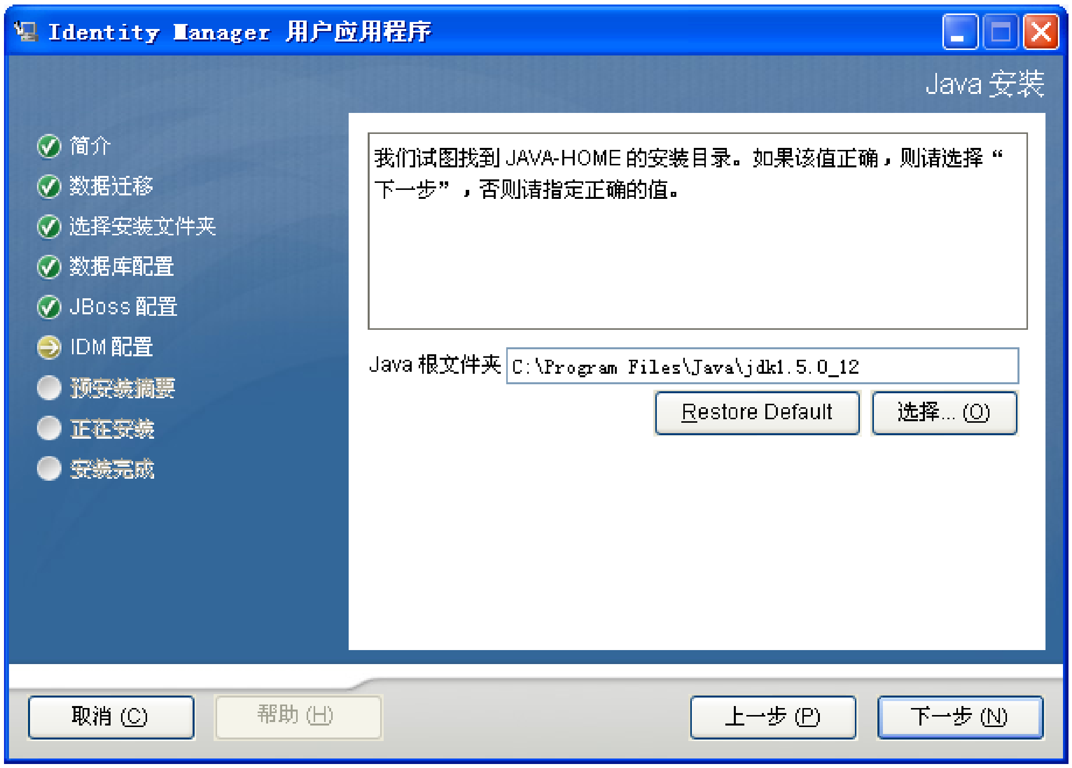


字段	说明
数据库名称（或 SID）	对于 MySQL 或 MS SQL Server，提供预配置数据库的名称。对于 Oracle，提供以前创建的 Oracle 系统标识符 (SID)。 对于群集，对其中每个成员指定相同的数据库名称或 SID。
数据库用户	指定数据库用户。 对于群集，对其中每个成员指定相同的数据库用户。
数据库口令 / 确认口令	指定数据库口令。 对于群集，对其中每个成员指定相同的数据库口令。

2 单击 *下一步*，然后继续第 5.5.9 节 “指定 Java 根目录”（第 116 页）。

5.5.9 指定 Java 根目录

1 单击*选择*浏览 Java 根文件夹。要使用默认位置，请单击*恢复默认值*。



2 单击*下一步*，然后继续第 5.5.10 节 “指定 JBoss 应用程序服务器设置”（第 116 页）。

5.5.10 指定 JBoss 应用程序服务器设置

在此页上，为 User Application 指定查找 JBoss 应用程序服务器的位置。

此安装过程不安装 JBoss 应用程序服务器：有关安装 JBoss 应用程序服务器的指导，请参见第 5.1.1 节 “安装 JBoss 应用程序服务器和 MySQL 数据库”（第 95 页）。

1 提供根文件夹、主机和端口：

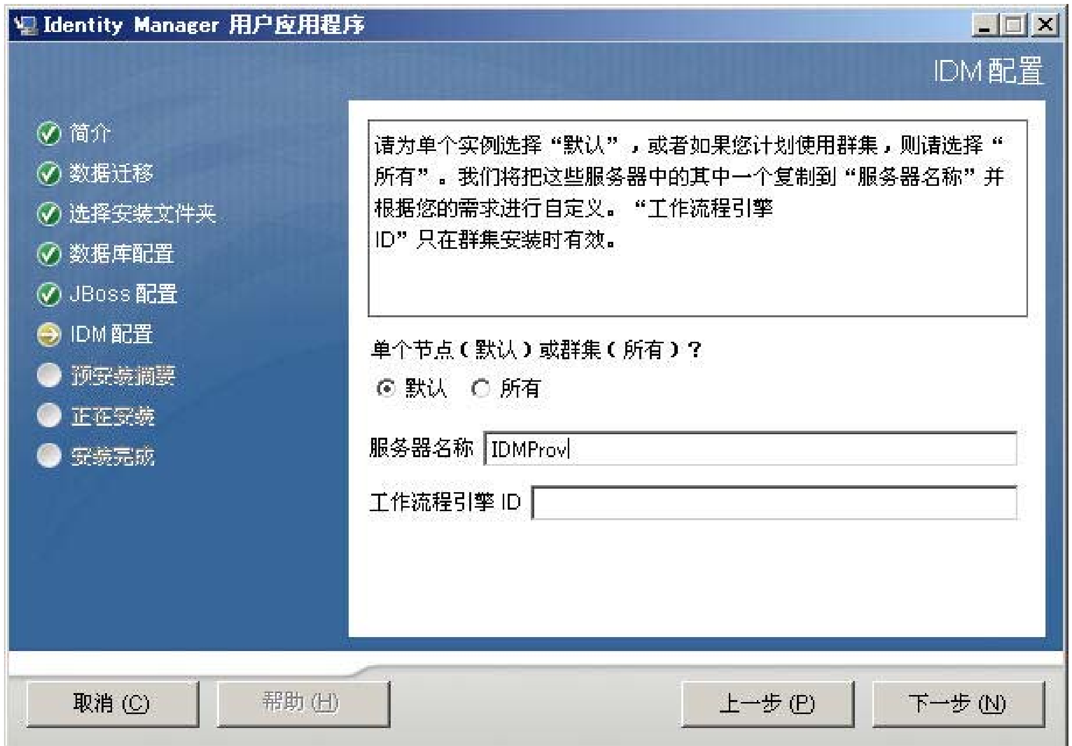


字段	说明
基本文件夹	指定应用程序服务器的位置。
主机	指定应用程序服务器的主机名或 IP 地址。
端口	指定应用程序服务器的侦听器端口号。JBoss 默认端口为 8080。

2 单击*下一步*，然后继续第 5.5.11 节 “选择应用程序服务器配置类型”（第 118 页）。

5.5.11 选择应用程序服务器配置类型

1 填写以下字段：



选项	说明
单个（默认）或*群集*（所有）	选择应用程序服务器配置的类型： ◆ 如果此安装是群集中的一部分，选择*全部* ◆ 如果此安装是单独节点，而不是群集的一部分，选择*默认值*
服务器名称	指定服务器名称。 服务器名称为应用程序服务器配置的名称、应用程序 WAR 文件的名称和 URL 环境的名称。安装底稿创建服务器配置，并默认根据*应用程序名称*命名配置。 将应用程序名称记录下来，当从浏览器启动 Identity Manager User Application 时，将其添加到 URL 中。
工作流程引擎 ID	群集中的每个服务器都必须具有唯一的工作流程引擎 ID。有关工作流程引擎 ID 的说明，请参见《*Identity Manager User Application：管理指南*》中的 3.5.4 部分：对群集配置工作流程。

2 单击*下一步*，然后继续第 5.5.12 节 “启用 Novell Audit 日志记录”（第 119 页）。

5.5.12 启用 Novell Audit 日志记录

（可选）要对 User Application 启用 Novell Audit 日志记录，请执行下列操作：

1 填写以下字段：



选项	说明
开	启用 User Application 的 Novell Audit 日志记录。 有关设置 Novell Audit 日志记录的更多信息，请参见 《*Identity Manager User Application：管理指南*》。
关	禁用 User Application 的 Novell Audit 日志记录。以后可以使用 User Application 的*管理*选项卡来启用该功能。 有关启用 Novell Audit 日志记录的更多信息，请参见 《*Identity Manager User Application：管理指南*》。
服务器	如果启用了 Novell Audit 日志记录，请指定 Novell Audit 服务器的主机名或 IP 地址。如果禁用日志记录，将忽略此值。

2 单击*下一步*，然后继续第 5.5.14 节 “配置 User Application”（第 121 页）。

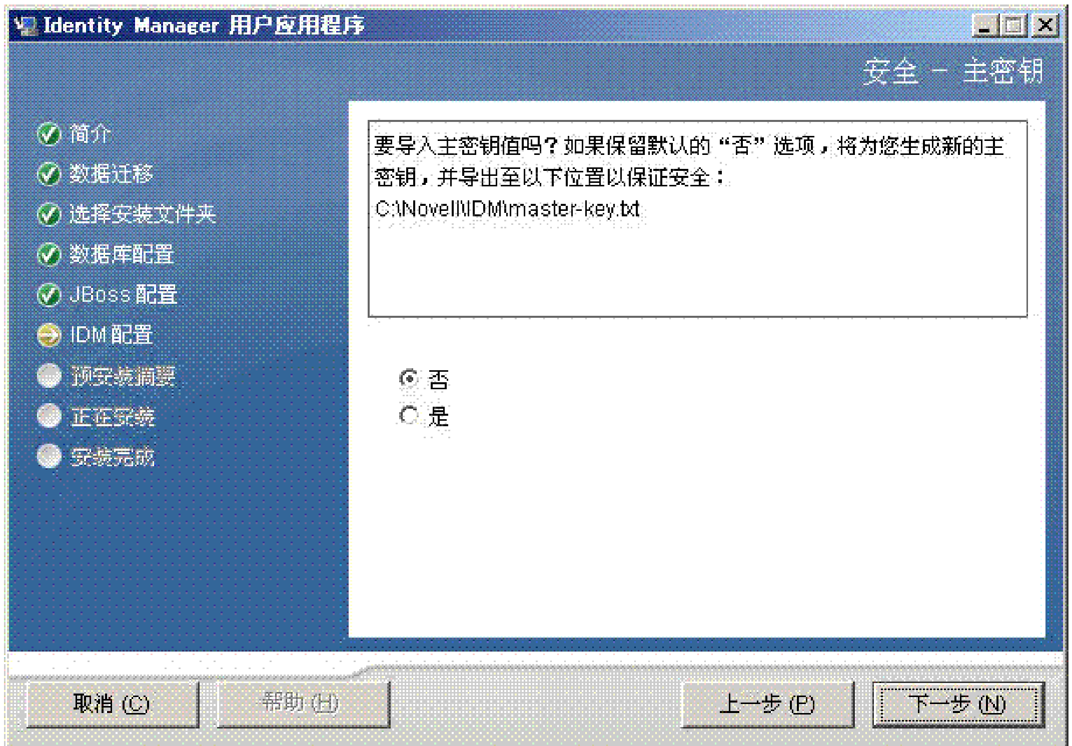
5.5.13 指定主密钥

指定是要导入现有主密钥还是新建主密钥。导入现有主密钥的情况例如：

- 将安装从临时系统移到生产系统，并想继续访问过去临时系统中使用的数据库。

- 已将 User Application 安装在 JBoss 群集中的第一个成员上，现在在群集中的后续成员上执行安装。
- 由于磁盘故障，需要恢复 User Application。必须重新安装 User Application，并指定以前安装过程中所使用的同一个经过加密的主密钥。这样可以获得以前存储的加密数据的访问权。

1 单击*是*导入现有主密钥，或者单击*否*新建主密钥。



2 单击*下一步*。

安装过程中会将经过加密的主密钥写到安装目录中的 master-key.txt 文件中。

如果选择*否*，跳至第 5.5.14 节 “配置 User Application”（第 121 页）。完成安装后，必须手动记录主密钥，如第 5.9.1 节 “记录主密钥”（第 163 页）中所述。

如果选择*是*，继续步骤 3。

3 如果选择导入现有经过加密的主密钥，请将密钥剪切和粘贴到安装过程窗口。



4 单击*下一步*并继续第 5.5.14 节 “配置 User Application”（第 121 页）。

5.5.14 配置 User Application

在 User Application 安装过程中，可以设置 User Application 配置参数。其中大部分参数都还可以于安装在 configupdate.sh 或 configupdate.bat 中进行配置，有关例外的项，参见参数说明中的注释。

对于群集，对其中每个成员指定相同的 User Application 配置参数。

1 设置基本 User Application 配置参数（参见表 5-4 中的说明），然后继续步骤 2。



表 5-4 User Application 配置：基本参数

设置类型	字段	说明
eDirectory 连接设置	*LDAP 主机*	必需。指定 LDAP 服务器的主机名或 IP 地址，及其安全端口。例如： `myLDAPhost`
	LDAP 非安全端口	为 LDAP 服务器指定非安全端口。例如：389。
	LDAP 安全端口	为 LDAP 服务器指定安全端口。例如：636。
	LDAP 管理员	必需。指定 LDAP 管理员的身份凭证。该用户必须已经存在。User Application 使用此帐户来建立与身份库 的管理连接。此值已使用主密钥进行过加密。
	LDAP 管理员口令	必需。指定 LDAP 管理员口令。此口令已使用主密钥进行过加密。
	使用公开匿名帐户	允许没有登录的用户访问 LDAP 公开匿名帐户。
	LDAP Guest	允许没有登录的用户访问允许的入口小程序。身份库 中必须已经存在此用户帐户。要启用 LDAP Guest，必须取消选择*使用公开匿名帐户*。要禁用 Guest 用户，请选择*使用公开匿名帐户*。
	LDAP Guest 口令	指定 LDAP Guest 口令。
	安全 Admin 连接	通过选中此选项，可以要求所有使用 Admin 帐户的通讯都通过安全套接字进行 （不选中此选项则相反）。
	安全用户连接	通过选中此选项，可以要求所有使用已登录 帐户的通讯都采用安全套接字执行 （不选中此选项则相反）。

设置类型	字段	说明
eDirectory DN	*根树枝 DN*	必需。指定根树枝的 LDAP 判别名。如果没有在目录抽象层中指定搜索根，则将该判别名用作默认的实体定义搜索根。
	供应驱动程序 DN	必需。指定以前在第 5.3 节 “创建 User Application 驱动程序”（第 100 页）中创建的 User Application 驱动程序的判别名。例如，如果驱动程序为 UserApplicationDriver，驱动程序集称为 MyDriverSet，并且驱动程序集位于环境 o=myCompany 中，则可以输入以下值： `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	User Application Admin	必需。身份库 中有权执行所指定 User Application 用户树枝的管理任务的现有用户。该用户可以使用 User Application 的*管理*选项卡管理入口。 如果 User Application 管理员参与 iManager、Designer for Identity Manager 或 User Application （*请求和批准*选项卡）中显示的工作流程管理任务，则必须授予此管理员对 User Application 驱动程序中包含的对象实例的相应受托者权利。有关细节，请参见 《*IDM User Application：管理指南*》。 要在部署 User Application 之后更改指派，必须使用 User Application 中的*管理* > *安全*页面。
	供应应用程序 Admin	Identity Manager 3.5.1 的供应版本中可以使用此角色。供应应用程序管理员使用*供应*选项卡（*管理*选项卡下方）来管理供应工作流程功能。用户可以通过 User Application 的*请求和批准*选项卡使用这些功能。在将用户指定为供应应用程序管理员之前，身份库 中必须存在此用户。 要在部署 User Application 之后更改指派，必须使用 User Application 中的*管理* > *安全*页面。
eDirectory DN（续）	*用户树枝 DN*	必需。指定用户树枝的 LDAP 判别名 (DN) 或完全限定的 LDAP 名称。这定义用户和组的搜索范围。允许该树枝中 （及其下）的用户登录 User Application。 **重要：**如果要使该用户能够执行工作流程，请确保在 User Application 驱动程序设置过程中指定的 User Application 管理员在该树枝中存在。
	组树枝 DN	必需。指定组树枝的 LDAP 判别名 (DN) 或完全限定的 LDAP 名称。 由目录抽象层中的实体定义使用。

设置类型	字段	说明
eDirectory 证书	*密钥存储区路径*	必需。指定应用程序服务器用于运行的、 JDK 密钥存储区 (cacerts) 文件的完整路径，或单击小浏览器按钮，然后浏览找到 cacerts 文件。 在 Linux 或 Solaris 上，用户必须具有写此文件的权限。
	密钥存储区口令 / 确认密钥存储区口令	必需。指定 cacerts 口令。默认值为 changeit。
电子邮件	*通知模板 Host 令牌*	指定主管 Identity Manager User Application 的应用程序服务器。例如： `myapplication serverServer` 此值将替换电子邮件模板中的 $HOST$ 令牌。所建立的 URL 是指向供应请求任务和批准通知的链接。
	通知模板 Port 令牌	用于替换供应请求任务和批准通知所用的电子邮件模板中的 $PORT$ 令牌。
	通知模板 Secure Port 令牌	用于替换供应请求任务和批准通知所用的电子邮件模板中的 $SECURE_PORT$ 令牌。
	通知 SMTP 电子邮件发件人：	指定供应电子邮件中发送邮件用户的电子邮件。
	通知 SMTP 电子邮件主机：	指定供应电子邮件所使用的 SMTP 电子邮件主机。这可以是 IP 地址或 DNS 名。
口令管理	*使用外部口令 WAR*	通过此功能，可以指定外部忘记口令 WAR 中的 “忘记口令” 页，或外部忘记口令 WAR 用于通过万维网服务回拨 User Application 的 URL。 如果选中*使用外部口令 WAR*，则必须提供*忘记口令链接*和*忘记口令返回链接*的值。 如果没有选择*使用外部口令 IDM*，则 IDM 将使用默认的内部口令管理功能。 /jsps/pwdmgt/ForgotPassword.jsf （开头没有 http(s) 协议）。这将用户重定向到内置于 User Application 的 “忘记口令” 功能，而不是外部 WAR。
	忘记口令链接	此 URL 指向 “忘记口令” 功能页。指定外部或内部口令管理 WAR 中的 ForgotPassword.jsf 文件。有关细节，请参见使用口令 WAR （第 131 页）。
	忘记口令返回链接	如果使用的是外部口令管理 WAR，需提供外部口令管理 WAR 用来通过万维网服务回调 User Application 的路径，例如 https://*idmhost*:*sslport*/idm。

2 如果要设置其他 User Application 配置参数，请单击*显示高级选项*。（通过滚动查看整个面板。）表 5-5 说明了 “高级选项” 参数。

如果不想设置此步骤中所述的其他参数，请跳至步骤 3。

表 5-5 User Application 配置：所有参数

设置类型	字段	说明
eDirectory 连接设置	*LDAP 主机*	必需。为 LDAP 服务器指定主机名或 IP 地址。例如： myLDAPhost
	LDAP 非安全端口	为 LDAP 服务器指定非安全端口。例如：389。
	LDAP 安全端口	为 LDAP 服务器指定安全端口。例如：636。
	LDAP 管理员	必需。指定 LDAP 管理员的身份凭证。该用户必须已经存在。User Application 使用此帐户来建立与身份库 的管理连接。此值已使用主密钥进行过加密。
	LDAP 管理员口令	必需。指定 LDAP 管理员口令。此口令已使用主密钥进行过加密。
	使用公开匿名帐户	允许没有登录的用户访问 LDAP 公开匿名帐户。
	LDAP Guest	允许没有登录的用户访问允许的入口小程序。身份库 中必须已经存在此用户帐户。要启用 LDAP Guest，必须取消选择*使用公开匿名帐户*。要禁用 Guest 用户，请选择*使用公开匿名帐户*。
	LDAP Guest 口令	指定 LDAP Guest 口令。
	安全 Admin 连接	通过选中此选项，可以要求所有使用 Admin 帐户的通讯都通过安全套接字进行 （不选中此选项则相反）。
	安全用户连接	通过选中此选项，可以要求所有使用已登录用户帐户的通讯都通过安全套接字进行 （不选中此选项则相反）。

设置类型	字段	说明
eDirectory DN	*根树枝 DN*	必需。指定根树枝的 LDAP 判别名。如果没有在目录抽象层中指定搜索根，则将该判别名用作默认的实体定义搜索根。
	供应驱动程序 DN	必需。指定以前在第 5.3 节 “创建 User Application 驱动程序”（第 100 页）中创建的 User Application 驱动程序的判别名。例如，如果驱动程序为 UserApplicationDriver，驱动程序集称为 myDriverSet，并且驱动程序集位于环境 o=myCompany 中，则可以输入以下值： `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	User Application Admin	必需。身份库 中有权执行所指定 User Application 用户树枝的管理任务的现有用户。该用户可以使用 User Application 的*管理*选项卡管理入口。 如果 User Application 管理员参与 iManager、Designer for Identity Manager 或 User Application （*请求和批准*选项卡）中显示的工作流程管理任务，则必须授予此管理员 User Application 驱动程序中包含的对象实例的相应受托者权限。有关细节，请参见 《*IDM User Application：管理指南*》。 要在部署 User Application 之后更改指派，必须使用 User Application 中的*管理* > *安全*页面。
	供应应用程序 Admin	Identity Manager 3.5.1 的供应版本中可以使用此角色。供应应用程序管理员管理 User Application 的*请求和批准*选项卡中可用的供应工作流程功能。在将用户指定为供应应用程序管理员之前，身份库 中必须存在此用户。 要在部署 User Application 之后更改指派，必须使用 User Application 中的*管理* > *安全*页面。

设置类型	字段	说明
元目录用户身份	*用户树枝 DN*	必需。指定用户树枝的 LDAP 判别名 (DN) 或完全限定的 LDAP 名称。 这定义用户和组的搜索范围。 允许该树枝中 （及其下）的用户登录 User Application。 **重要：**如果要使该用户能够执行工作流程，请确保在 User Application 驱动程序设置过程中指定的 User Application 管理员在该树枝中存在。
	用户对象类	LDAP 用户对象类 （通常为 inetOrgPerson）。
	登录属性	代表用户的登录名的 LDAP 属性 （比如 CN）。
	命名属性	用作查找用户或组时的标识符的 LDAP 属性。这不同于登录属性，登录属性仅在登录时使用，在用户 / 组搜索时不使用。
	用户成员资格属性	可选。代表用户的组成员资格的 LDAP 属性。不要在该名称中使用空格。
元目录用户组	*组树枝 DN*	必需。指定组树枝的 LDAP 判别名 (DN) 或完全限定的 LDAP 名称。由目录抽象层中的实体定义使用。
	组对象类	LDAP 组对象类 （通常是 groupofNames）。
	组成员资格属性	代表用户组成员资格的属性。不要在该名称中使用空格。
	使用动态组	如果需要使用动态组，请选择该选项。
	动态组对象类	LDAP 动态组对象类 （一般 dynamicGroup）。
eDirectory 证书	*密钥存储区路径*	必需。指定应用程序服务器用于运行的 JRE 的密钥存储区 (cacerts) 文件的完整路径，或单击浏览器按钮，然后浏览找到 cacerts 文件。 User Application 安装过程中将修改密钥存储区文件。在 Linux 或 Solaris 上，用户必须具有写此文件的权限。
	密钥存储区口令	必需。指定 cacerts 口令。默认值为 changeit。
	确认密钥存储区口令	
私用密钥存储区	*私用密钥存储区路径*	私用密钥存储区包含 User Application 的私用密钥和证书。保留 . 如果保留为空的话，将采用默认路径 /jre/lib/security/cacerts。
	私用密钥存储区口令	口令为 changeit，除非另行指定。此口令已使用主密钥进行过加密。
	私用密钥别名	别名为 novellIDMUserApp，除非另行指定。
	私用密钥口令	口令为 novellIDM，除非另行指定。此口令已使用主密钥进行过加密。

设置类型	字段	说明
可信密钥存储区	*可信存储区路径*	可信密钥存储区包含所有用于验证数字签名的可信签名者的证书。如果此路径为空的话，User Application 将从系统属性 javax.net.ssl.trustStore 中获取路径。如果那里没有路径，则假定为 jre/lib/security/cacerts。
	可信存储口令	如果此字段为空的话，User Application 将从系统属性 javax.net.ssl.trustStorePassword 中获取口令。如果那里没有值，则使用 changeit。此口令已使用主密钥进行过加密。
Novell Audit 数字签名和证书密钥		包容 Novell Audit 数字签名密钥和证书。
	Novell Audit 数字签名证书	显示数字签名证书。
	Novell Audit 数字签名私用密钥	显示数字签名私用密钥。此密钥已使用主密钥进行过加密。
iChain 设置	*已启用 ICS 注销*	如果选中了此选项，则 User Application 支持同时注销 User Application 和 iChain® 或 Novell Access Manager。注销时，User Application 检查是否存在 iChain 或 Novell Access Manager Cookie，如果存在 Cookie，则将用户重路由到 ICS 注销页。
	ICS 注销页	iChain 或 Novell Access Manager 注销页的 URL，其中该 URL 是 iChain 或 Novell Access Manager 预期的主机名。如果启用了 ICS 日志记录并且用户要注销 User Application，则将用户重路由到此页面。

设置类型	字段	说明
电子邮件	*通知模板 Host 令牌*	指定主管 Identity Manager User Application 的应用程序服务器。例如： `myapplication serverServer` 此值将替换电子邮件模板中的 $HOST$ 令牌。所建立的 URL 是指向供应请求任务和批准通知的链接。
	通知模板 Port 令牌	用于替换供应请求任务和批准通知所用的电子邮件模板中的 $PORT$ 令牌。
	通知模板 Secure Port 令牌	用于替换供应请求任务和批准通知所用的电子邮件模板中的 $SECURE_PORT$ 令牌。
	通知模板 PROTOCOL 令牌	指非安全协议 HTTP。用于替换供应请求任务和批准通知所用的电子邮件模板中的 $PROTOCOL$ 令牌。
	通知模板 SECURE PROTOCOL 令牌	指安全协议 HTTPS。用于替换供应请求任务和批准通知所使用电子邮件模板中的 $SECURE_PROTOCOL$ 令牌。
	通知 SMTP 电子邮件发件人：	指定供应电子邮件中发送电子邮件的用户。
	通知 SMTP 电子邮件主机：	指定供应电子邮件所使用的 SMTP 电子邮件主机。这可以是 IP 地址或 DNS 名。
口令管理		
	使用外部口令 WAR	通过此功能，可以指定外部忘记口令 WAR 中的“忘记口令”页，或外部忘记口令 WAR 用于通过万维网服务回拨 User Application 的 URL。 如果选择*使用外部口令 WAR*，**则必须提供***忘记口令链接***和***忘记口令返回链接*的值。 如果没有选择*使用外部口令 WAR*，则 IDM 将使用默认的内部口令管理功能。 /jsps/pwdmgt/ForgotPassword.jsf （开头没有 http(s) 协议）。这将用户重定向到内置于 User Application 的 “忘记口令”功能，而不是外部 WAR。
	忘记口令链接	此 URL 指向 “忘记口令”功能页。指定外部或内部口令管理 WAR 中的 ForgotPassword.jsf 文件。有关细节，请参见使用口令 WAR（第 131 页）。
	忘记口令返回链接	如果使用的是外部口令管理 WAR，需提供外部口令管理 WAR 用来通过万维网服务回调 User Application 的路径，例如 https://*idmhost:sslport*/idm。

设置类型	字段	说明
杂项	*会话超时*	应用程序会话超时。
	OCSP URI	如果客户安装使用在线证书状态协议 (OCSP)，请提供统一资源标识符 (URI)。例如，格式为 http://host:port/ocspLocal。 OCSP URI 在线更新可信证书的状态。
	授权配置路径	授权配置文件的完全限定名。
树枝对象	*所选*	选择要使用的每个数字对象类型。
	树枝对象类型	有以下标准树枝可供选择：位置、国家 / 地区、组织单位、组织和域。也可以在 iManager 中自己定义树枝，然后在*添加新树枝对象*下面添加这些树枝。
	树枝属性名称	列出与树枝对象类型相关的属性类型名称。
	添加新的树枝对象：树枝对象类型	指定可作为树枝的身份库 中的对象类的 LDAP 名称。 有关树枝的信息，请参见 《*Novell iManager 2.6 管理指南 (http://www.novell.com/documentation/imanager26/pdfdoc/imanager_admin_26/imanager_admin_26.pdf)*》。
	添加新的树枝对象：树枝属性名称	提供树枝对象的属性名称。

注释 : 安装后，可以编辑此文件中的大部分设置。要执行此操作，请运行安装子目录中的 configupdate.sh 底稿或 Windows configupdate.bat 文件。请记住，在群集中，此文件中的设置对于群集中的所有成员必须保持一致。

3 完成设置配置之后，单击*确定*，然后继续第 5.5.15 节 “校验选择并安装”（第 132 页）。

使用口令 WAR

通过*忘记口令链接*配置参数，可以指定包含 “忘记口令”功能的 WAR 的位置。可以对 User Application 指定外部或内部 WAR。

指定外部口令管理 WAR

1 使用安装过程或 configupdate 实用程序。

2 在 User Application 配置参数中，选中*使用外部口令 WAR* 配置参数复选框。

3 对于*忘记口令链接*配置参数，指定外部口令 WAR 的位置。

包括主机和端口，比如 http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf。外部口令 WAR 可以位于保护 User Application 的防火墙之外。

4 对于*忘记口令返回链接*，需提供外部口令管理 WAR 用于通过万维网服务回调 User Application 的路径，比如 https:// *idmhost:sslport*/idm。

返回链接必须使用 SSL，以确保与 User Application 进行安全万维网服务通讯。另请参见第 5.9.3 节 “配置 JBoss 服务器之间的 SSL 通讯”（第 164 页）。

5 如果使用了安装程序，请阅读此步骤中的信息，然后继续步骤 6。

如果使用 configupdate 实用程序更新安装根目录中的外部口令 WAR，请阅读此步骤并手动将 WAR 重命名为在*忘记口令链接*中指定的第一个目录。然后，继续步骤 6。

在安装结束之前，安装程序将 IDMPwdMgt.war （安装程序中附带）重命名为指定的第一个目录。经过重命名的 IDMPwdMgt.war 称为外部口令 WAR。例如，如果指定的是 http://www.idmpwdmgthost.com/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf，安装程序会将 IDMPwdMgt.war 重命名为 ExternalPwd.war。安装程序将重命名过的 WAR 移至安装根目录。

6 手动将 ExternalPwd.war 复制到运行外部口令 WAR 功能的远程 JBoss 服务器部署目录。

指定内部口令管理 WAR

1 不要选择*使用外部口令 WAR*。
2 接受*忘记口令链接*的默认位置，或者提供另一个口令 WAR 的 URL。
3 接受*忘记口令返回链接*的默认值。

5.5.15 校验选择并安装

1 阅读 “安装前摘要”页，校验所选择的安装参数。
2 如有必要，使用*后退*返回到前面的安装页，对安装参数作出更改。

   User Application 配置页的值没有保存下来，因此，在重新指定安装中的以前页面之后，必须重新输入 User Application 配置值。

3 当安装和配置参数满意之后，返回 “安装前摘要”页，然后单击*安装*。

5.5.16 查看日志文件

1 如果安装成功完成，没有错误，请转至第 5.9 节 “安装后的任务”（第 163 页）。
2 如果安装提示出现错误或警告，请检查日志忘记以确定问题：
   - Identity_Manager_User_Application_InstallLog.log 保存基本安装任务的结果
   - Novell-Custom-Install.log 记录了有关安装过程中所执行的 User Application 配置

   欲获得解决问题的帮助，请参见第 5.11 节 “查错”（第 167 页）。

5.6 在 WebSphere 应用程序服务器上安装 User Application

本部分说明如何在 WebSphere 应用程序服务器上通过安装程序的图形用户界面版本安装 IDM User Application。

- 第 5.6.1 节 “起动安装程序 GUI”（第 133 页）
- 第 5.6.2 节 “选择应用程序服务器平台”（第 134 页）
- 第 5.6.3 节 “指定 WAR 的位置”（第 135 页）
- 第 5.6.4 节 “选择安装文件夹”（第 137 页）
- 第 5.6.5 节 “选择数据库平台”（第 138 页）
- 第 5.6.6 节 “指定 Java 根目录”（第 140 页）

- 第 5.6.7 节 “启用 Novell Audit 日志记录”（第 141 页）
- 第 5.6.8 节 “指定主密钥”（第 142 页）
- 第 5.6.9 节 “配置 User Application”（第 144 页）
- 第 5.6.10 节 “校验选择并安装”（第 154 页）
- 第 5.6.11 节 “查看日志文件”（第 155 页）
- 第 5.6.12 节 “添加 User Application 配置文件和 JVM 系统属性”（第 155 页）
- 第 5.6.13 节 “将 eDirectory 可信根导入 WebSphere 密钥存储区”（第 156 页）
- 第 5.6.14 节 “部署 IDM WAR 文件”（第 157 页）
- 第 5.6.15 节 “启动应用程序”（第 157 页）
- 第 5.6.16 节 “访问 User Application 门户”（第 157 页）

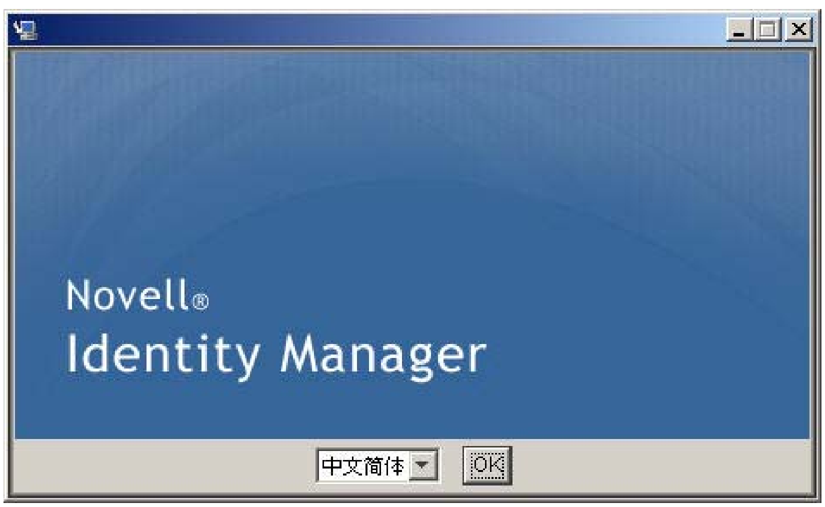
5.6.1 起动安装程序 GUI

1 浏览找到包含安装文件的目录。

2 起动安装程序：

java -jar IdmUserApp.jar

3 从下拉菜单中选择一种语言，然后单击 “确定”。



4 阅读许可证协议，单击*我接受许可证协议中的条款*，然后单击*下一步*。



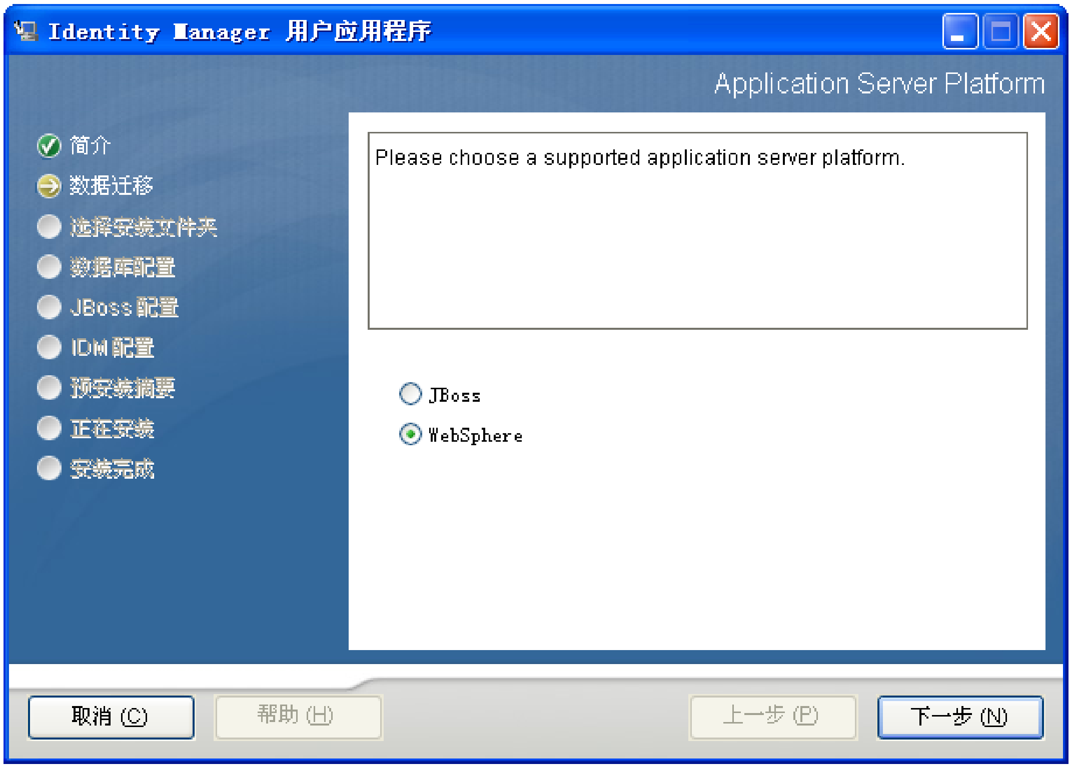
5 阅读安装向导的 “介绍”页，然后单击*下一步*。

6 继续第 5.6.2 节 “选择应用程序服务器平台”（第 134 页）。

5.6.2 选择应用程序服务器平台

1 在 “应用程序服务器平台”窗口中，选择 WebSphere 应用程序服务器平台。

2 选择*下一步*。然后继续第 5.6.3 节 “指定 WAR 的位置”（第 135 页）。

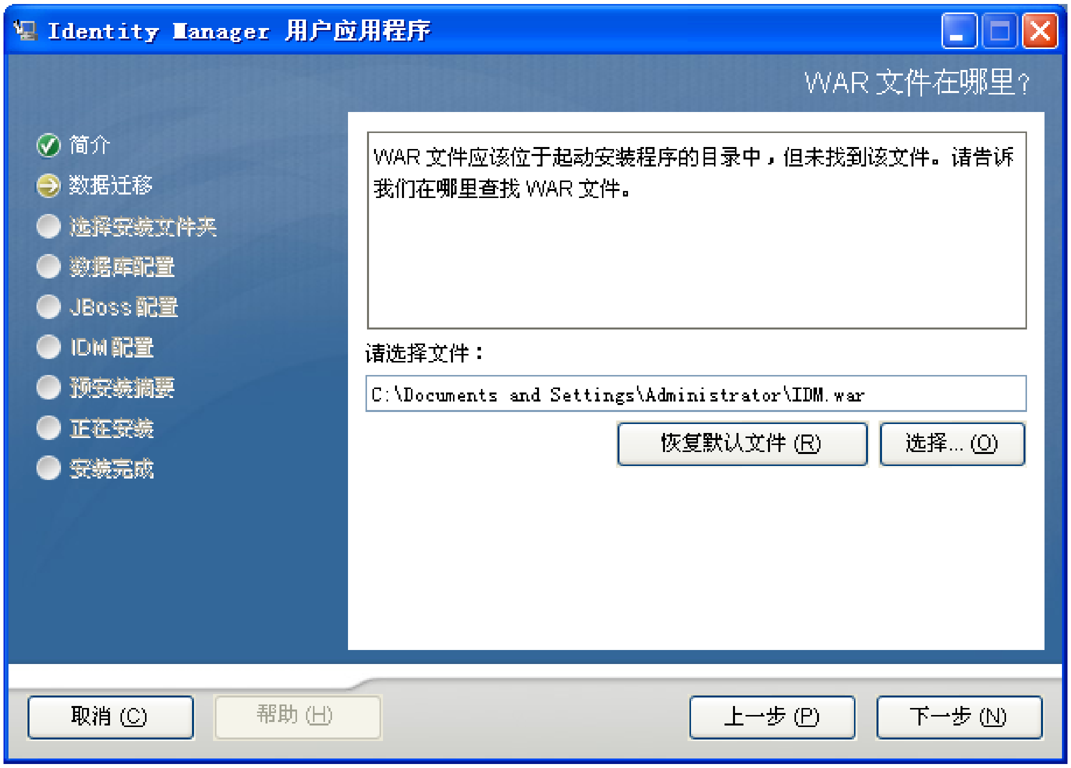


5.6.3 指定 WAR 的位置

如果 Identity Manager User Application WAR 文件所在的目录不同于安装程序，安装程序将提示提供 WAR 的路径。

1 如果 WAR 在默认位置，可以单击*恢复默认文件夹*。

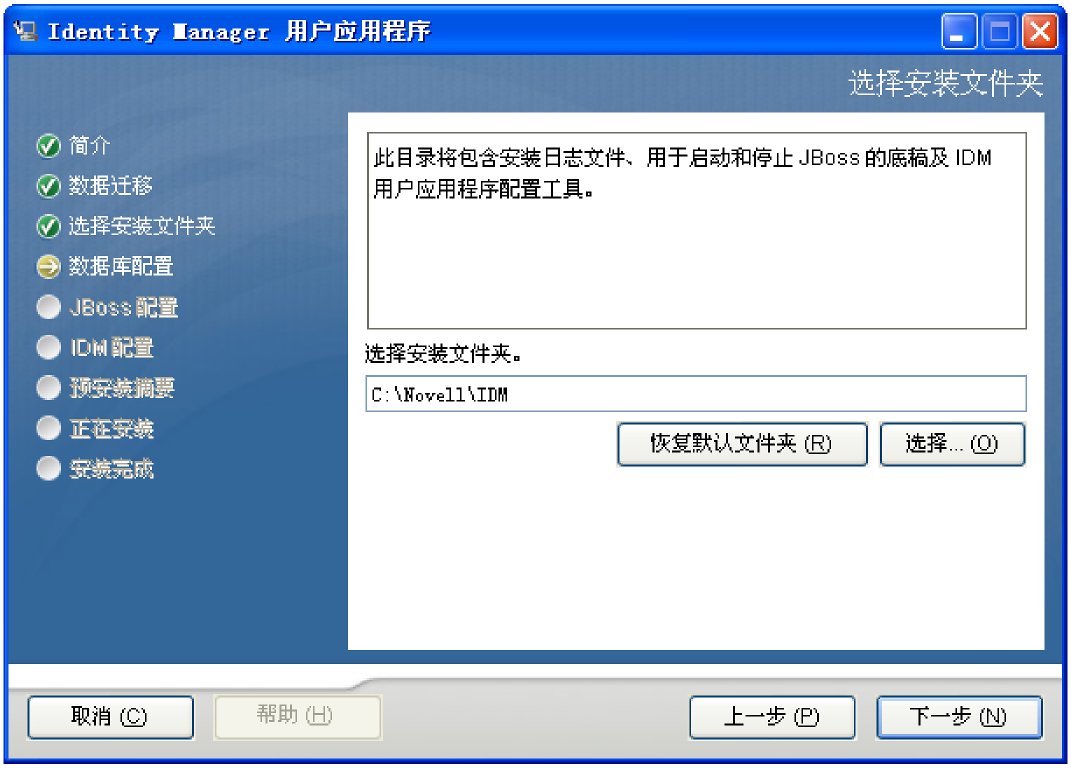
或者，要指定 WAR 文件的位置，单击*选择*并选择某个位置。



2 单击*下一步*，然后继续第 5.6.4 节 “选择安装文件夹”（第 137 页）。

5.6.4 选择安装文件夹

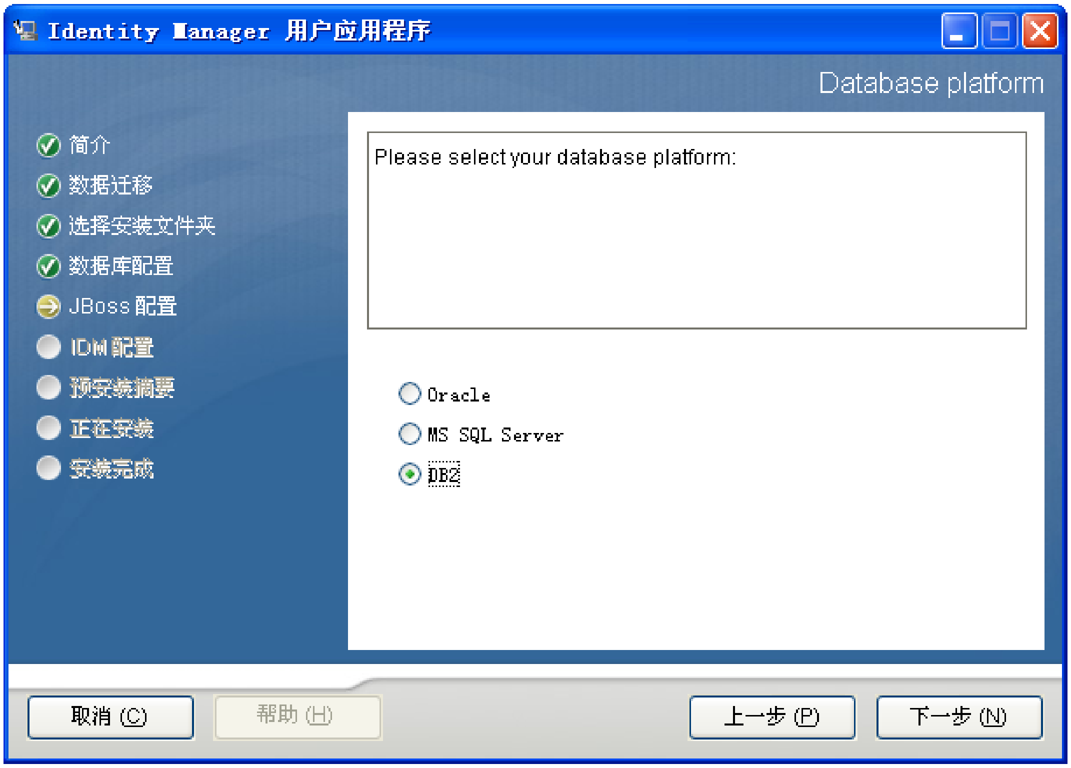
1 在“选择安装文件夹”页，选择安装 User Application 的位置。如果使用默认位置，单击*恢复默认文件夹*；如果要为安装文件选择其他位置，单击*选择*并浏览某个位置。



2 单击*下一步*，然后继续第 5.6.5 节 “选择数据库平台”（第 138 页）。

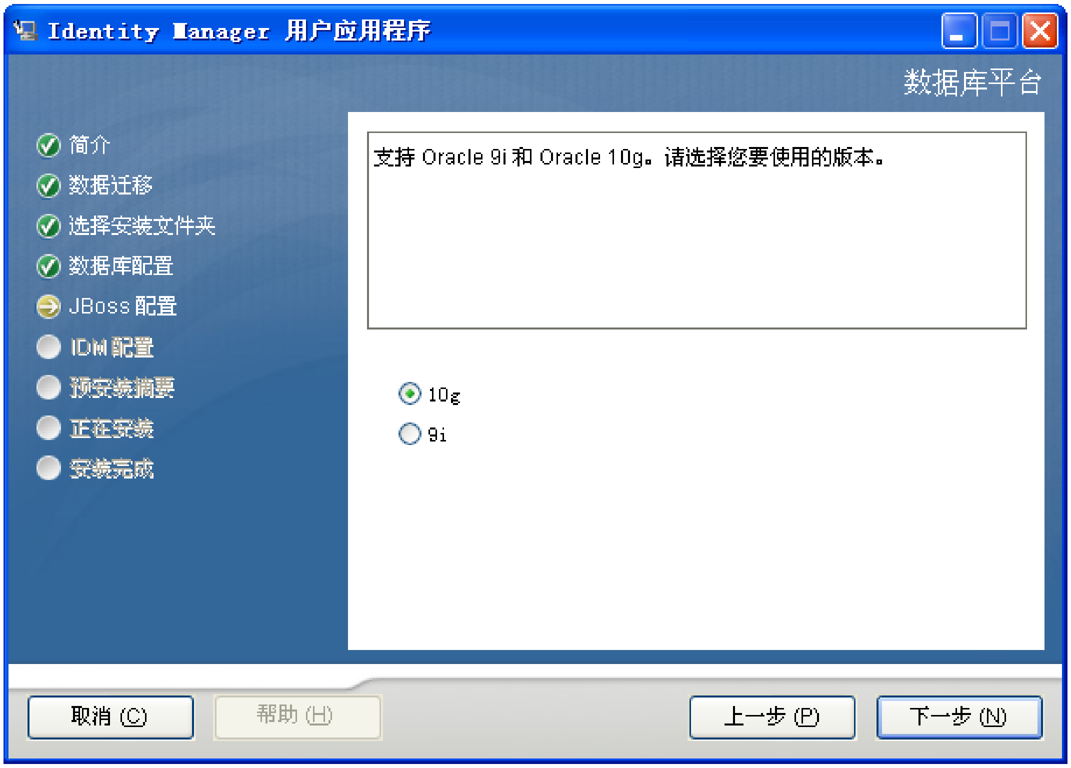
5.6.5 选择数据库平台

1 选择要使用的数据库平台。



2 如果使用的是 Oracle 数据库，请继续步骤 3。否则，请跳至步骤 4。

3 如果使用的是 Oracle 数据库，安装程序将询问所使用的版本。选择使用的版本。



4 单击*下一步*，然后继续第 5.6.6 节 “指定 Java 根目录”（第 140 页）。

5.6.6 指定 Java 根目录

注释 : 对于 WebSphere，必须使用应用了无限制策略文件的 IBM JDK。

1 单击*选择*浏览 Java 根文件夹。要使用默认位置，请单击*恢复默认值*。



2 单击*下一步*，然后继续第 5.6.7 节 "启用 Novell Audit 日志记录"（第 141 页）。

5.6.7 启用 Novell Audit 日志记录

要启用 User Application 的 Novell Audit 日志记录（可选），请执行下列操作：

1 填写以下字段：



选项	说明
关	禁用 User Application 的 Novell Audit 日志记录。以后可以使用 User Application 的*管理*选项卡来启用该功能。 有关启用 Novell Audit 日志记录的更多信息，请参见 《*Identity Manager User Application：管理指南*》。
开	启用 User Application 的 Novell Audit 日志记录。 有关设置 Novell Audit 日志记录的更多信息，请参见 《*Identity Manager User Application：管理指南*》。
服务器	如果启用了 Novell Audit 日志记录，请指定 Novell Audit 服务器的主机名或 IP 地址。如果禁用日志记录，将忽略此值。
日志超速缓存文件夹	指定日志记录超速缓存的目录。

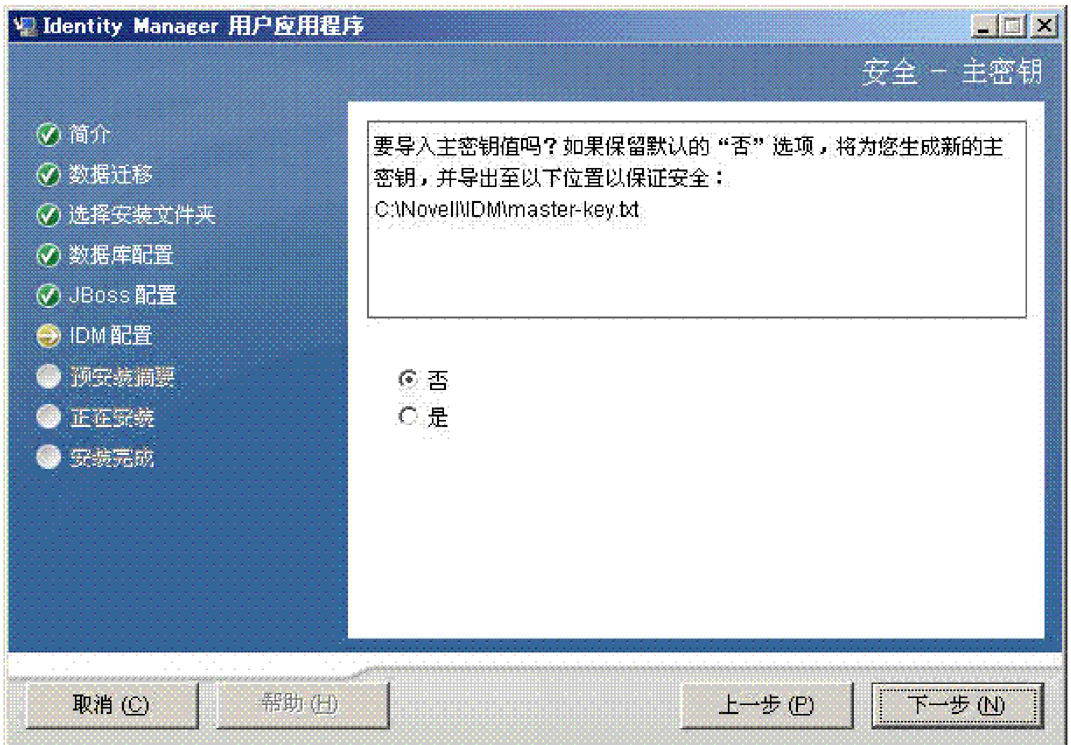
2 单击*下一步*并继续第 5.6.8 节 “指定主密钥”（第 142 页）。

5.6.8 指定主密钥

指定是要导入现有主密钥还是新建主密钥。导入现有主密钥的情况例如：

- 将安装从临时系统移到生产系统，并想继续访问过去临时系统中使用的数据库。
- 已将 User Application 安装在群集中的第一个成员上，现在在群集中的后续成员上执行安装 （它们需要同一主密钥）。
- 由于磁盘故障，需要恢复 User Application。必须重新安装 User Application，并指定以前安装过程中所使用的同一个经过加密的主密钥。这样可以获得以前存储的加密数据的访问权。

1 单击*是*导入现有主密钥，或者单击*否*新建主密钥。



2 单击*下一步*。

安装过程中会将经过加密的主密钥写到安装目录中的 master-key.txt 文件中。

如果选择*否*，跳至第 5.6.9 节 “配置 User Application”（第 144 页）。完成安装后，必须手动记录主密钥。如果选择*是*，则继续步骤 3。

3 如果选择导入现有经过加密的主密钥，请将密钥剪切和粘贴到安装过程窗口。

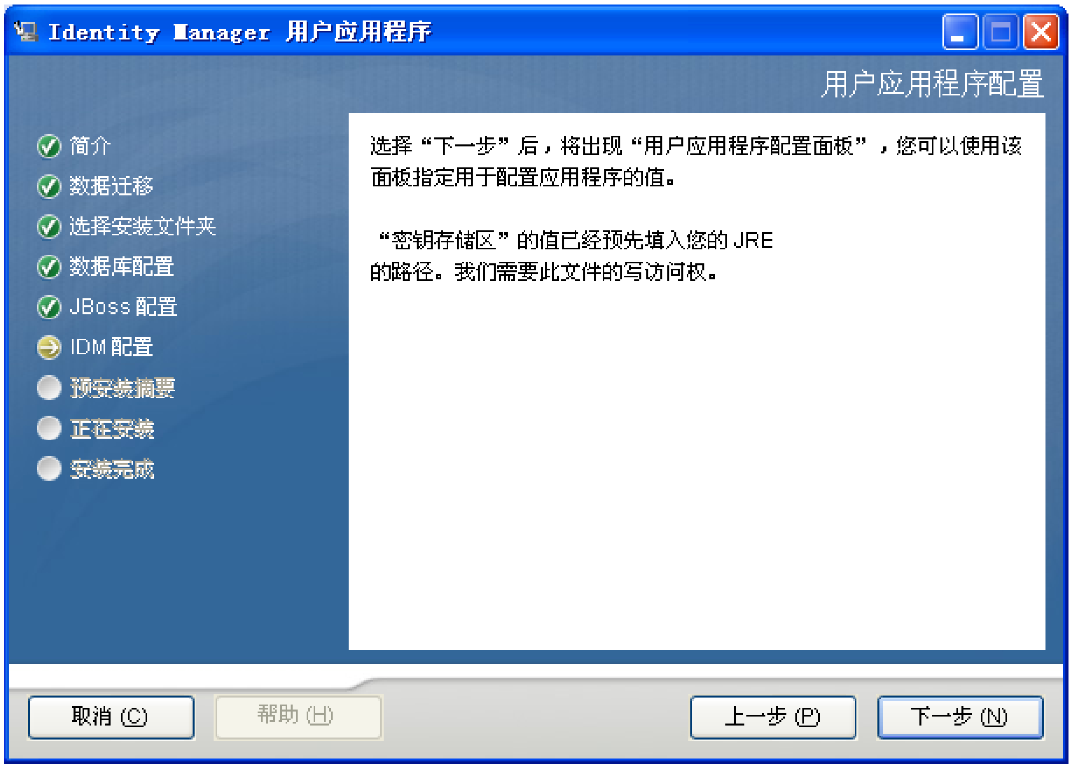


4 单击*下一步*并继续第 5.6.9 节 “配置 User Application”（第 144 页）。

5.6.9 配置 User Application

在 User Application 安装过程中，可以设置 User Application 配置参数。其中大部分参数都还可以于安装后在 configupdate.sh 或 configupdate.bat 中进行配置，有关例外的项，参见参数说明中的注释。对于群集，对其中每个成员指定相同的 User Application 配置参数。

1 单击 *下一步*完成首个 “User Application 配置” 页。



2 设置基本 User Application 配置参数（参见表 5-6（第 146 页）中的说明），然后继续步骤 3。



表 5-6 User Application 配置：基本参数

设置类型	字段	说明
eDirectory 连接设置	*LDAP 主机*	必需。指定 LDAP 服务器的主机名或 IP 地址，及其安全端口。例如： `myLDAPhost`
	LDAP 非安全端口	为 LDAP 服务器指定非安全端口。例如：389。
	LDAP 安全端口	为 LDAP 服务器指定安全端口。例如：636。
	LDAP 管理员	必需。指定 LDAP 管理员的身份凭证。该用户必须已经存在。User Application 使用此帐户来建立与身份库 的管理连接。此值已使用主密钥进行过加密。
	LDAP 管理员口令	必需。指定 LDAP 管理员口令。此口令已使用主密钥进行过加密。
	使用公开匿名帐户	允许没有登录的用户访问 LDAP 公开匿名帐户。
	LDAP Guest	允许没有登录的用户访问允许的入口小程序。身份库 中必须已经存在此用户帐户。要启用 LDAP Guest，必须取消选择*使用公开匿名帐户*。要禁用 Guest 用户，请选择*使用公开匿名帐户*。
	LDAP Guest 口令	指定 LDAP Guest 口令。
	安全 Admin 连接	通过选中此选项，可以要求所有使用 Admin 帐户的通讯都通过安全套接字进行 （不选中此选项则相反）。
	安全用户连接	通过选中此选项，可以要求所有使用已登录 帐户的通讯都采用安全套接字执行 （不选中此选项则相反）。

设置类型	字段	说明
eDirectory DN	*根树枝 DN*	必需。指定根树枝的 LDAP 判别名。如果没有在目录抽象层中指定搜索根，则将该判别名用作默认的实体定义搜索根。
	供应驱动程序 DN	必需。指定 User Application 驱动程序的判别名。例如，如果驱动程序为 UserApplicationDriver，驱动程序集称为 MyDriverSet，并且驱动程序集位于环境 o=myCompany 中，则可以输入以下值： `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	User Application Admin	必需。身份库 中有权执行所指定 User Application 用户树枝的管理任务的现有用户。该用户可以使用 User Application 的*管理*选项卡管理入口。 如果 User Application 管理员参与 iManager、Novell Designer for Identity Manager 或 User Application （*请求和批准*选项卡）中显示的工作流程管理任务，则必须授予此管理员对 User Application 驱动程序中包含的对象实例的相应受托者权限。有关细节，请参见 《*IDM User Application：管理指南*》。 要在部署 User Application 之后更改指派，必须使用 User Application 中的*管理* > *安全*页面。
	供应应用程序 Admin	Identity Manager 3.5.1 的供应版本中可以使用此角色。供应应用程序管理员使用*供应*选项卡（*管理*选项卡下方）来管理供应工作流程功能。用户可以通过 User Application 的*请求和批准*选项卡使用这些功能。在将用户指定为供应应用程序管理员之前，身份库 中必须存在此用户。 要在部署 User Application 之后更改指派，必须使用 User Application 中的*管理* > *安全*页面。
eDirectory DN （续）	*用户树枝 DN*	必需。指定用户树枝的 LDAP 判别名 (DN) 或完全限定的 LDAP 名称。这定义用户和组的搜索范围。允许该树枝中 （及其下）的用户登录 User Application。 **重要 :** 如果要使该用户能够执行工作流程，请确保在 User Application 驱动程序设置过程中指定的 User Application 管理员在该树枝中存在。
	组树枝 DN	必需。指定组树枝的 LDAP 判别名 (DN) 或完全限定的 LDAP 名称。 由目录抽象层中的实体定义使用。

设置类型	字段	说明
eDirectory 证书	*密钥存储区路径*	必需。指定应用程序服务器用于运行的、JDK 密钥存储区 (cacerts) 文件的完整路径，或单击小浏览器按钮，然后浏览找到 cacerts 文件。 在 Linux 或 Solaris 上，用户必须具有写此文件的权限。
	密钥存储区口令 / 确认密钥存储区口令	必需。指定 cacerts 口令。默认值为 changeit。
电子邮件	*通知模板 Host 令牌*	指定主管 Identity Manager User Application 的应用程序服务器。例如： `myapplication serverServer` 此值将替换电子邮件模板中的 $HOST$ 令牌。所建立的 URL 是指向供应请求任务和批准通知的链接。
	通知模板 Port 令牌	用于替换供应请求任务和批准通知所用的电子邮件模板中的 $PORT$ 令牌。
	通知模板 Secure Port 令牌	用于替换供应请求任务和批准通知所用的电子邮件模板中的 $SECURE_PORT$ 令牌。
	通知 SMTP 电子邮件发件人：	指定供应电子邮件中发送邮件用户的电子邮件。
	通知 SMTP 电子邮件主机：	指定供应电子邮件所使用的 SMTP 电子邮件主机。这可以是 IP 地址或 DNS 名。
口令管理	*使用外部口令 WAR*	通过此功能，可以指定外部忘记口令 WAR 中的 “忘记口令”页，或外部忘记口令 WAR 用于通过万维网服务回拨 User Application 的 URL。 如果选择*使用外部口令 WAR*，**则必须提供***忘记口令链接*和*忘记口令返回链接*的值。 如果没有选择*使用外部口令 WAR*，则 IDM 将使用默认的内部口令管理功能。/jsps/pwdmgt/ForgotPassword.jsf （开头没有 http(s) 协议）。这将用户重定向到内置于 User Application 的 “忘记口令”功能，而不是外部 WAR。
	忘记口令链接	此 URL 指向 “忘记口令”功能页。指定外部或内部口令管理 WAR 中的 ForgotPassword.jsf 文件。
	忘记口令返回链接	如果使用的是外部口令管理 WAR，需提供外部口令管理 WAR 用来通过万维网服务回调 User Application 的路径，例如 https://*idmhost*:*sslport*/idm。

3 如果要设置其他 User Application 配置参数，请单击*显示高级选项*。（通过滚动查看整个面板。）表 5-7 （第 149 页）说明了 “高级选项”参数。如果不想设置此步骤中所述的其他参数，请跳至步骤 4。

表 5-7 User Application 配置：所有参数

设置类型	字段	说明
eDirectory 连接设置	*LDAP 主机*	必需。为 LDAP 服务器指定主机名或 IP 地址。例如： myLDAPhost
	LDAP 非安全端口	为 LDAP 服务器指定非安全端口。例如：389。
	LDAP 安全端口	为 LDAP 服务器指定安全端口。例如：636。
	LDAP 管理员	必需。指定 LDAP 管理员的身份凭证。该用户必须已经存在。User Application 使用此帐户来建立与身份库 的管理连接。此值已使用主密钥进行过加密。
	LDAP 管理员口令	必需。指定 LDAP 管理员口令。此口令已使用主密钥进行过加密。
	使用公开匿名帐户	允许没有登录的用户访问 LDAP 公开匿名帐户。
	LDAP Guest	允许没有登录的用户访问允许的入口小程序。身份库 中必须已经存在此用户帐户。要启用 LDAP Guest，必须取消选择*使用公开匿名帐户*。要禁用 Guest 用户，请选择*使用公开匿名帐户*。
	LDAP Guest 口令	指定 LDAP Guest 口令。
	安全 Admin 连接	通过选中此选项，可以要求所有使用 Admin 帐户的通讯都通过安全套接字进行 （不选中此选项则相反）。
	安全用户连接	通过选中此选项，可以要求所有使用已登录用户帐户的通讯都通过安全套接字进行 （不选中此选项则相反）。

设置类型	字段	说明
eDirectory DN	*根树枝 DN*	必需。指定根树枝的 LDAP 判别名。如果没有在目录抽象层中指定搜索根，则将该判别名用作默认的实体定义搜索根。
	供应驱动程序 DN	必需。指定 User Application 驱动程序的判别名。例如，如果驱动程序为 UserApplicationDriver，驱动程序集称为 myDriverSet，并且驱动程序集位于环境 o=myCompany 中，则可以输入以下值： `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	User Application Admin	必需。身份库 中有权执行所指定 User Application 用户树枝的管理任务的现有用户。该用户可以使用 User Application 的*管理*选项卡管理入口。 如果 User Application 管理员参与 iManager、Designer for Identity Manager 或 User Application （*请求和批准*选项卡）中显示的工作流程管理任务，则必须授予此管理员对 User Application 驱动程序中包含的对象实例的相应受托者权限。有关细节，请参见 《*IDM User Application：管理指南*》。 要在部署 User Application 之后更改指派，必须使用 User Application 中的*管理* > *安全*页面。
	供应应用程序 Admin	Identity Manager 3.5.1 的供应版本中可以使用此角色。供应应用程序管理员管理 User Application 的*请求和批准*选项卡中可用的供应工作流程功能。在将用户指定为供应应用程序管理员之前，身份库 中必须存在此用户。 要在部署 User Application 之后更改指派，必须使用 User Application 中的*管理* > *安全*页面。

设置类型	字段	说明
元目录用户身份	*用户树枝 DN*	必需。指定用户树枝的 LDAP 判别名 (DN) 或完全限定的 LDAP 名称。 这定义用户和组的搜索范围。 允许该树枝中 （及其下）的用户登录 User Application。 **重要 :** 如果要使该用户能够执行工作流程，请确保在 User Application 驱动程序设置过程中指定的 User Application 管理员在该树枝中存在。
	用户对象类	LDAP 用户对象类 （通常为 inetOrgPerson）。
	登录属性	代表用户的登录名的 LDAP 属性 （比如 CN）。
	命名属性	用作查找用户或组时的标识符的 LDAP 属性。这不同于登录属性，登录属性仅在登录时使用，在用户 / 组搜索时不使用。
	用户成员资格属性	可选。代表用户的组成员资格的 LDAP 属性。不要在该名称中使用空格。
元目录用户组	*组树枝 DN*	必需。指定组树枝的 LDAP 判别名 (DN) 或完全限定的 LDAP 名称。由目录抽象层中的实体定义使用。
	组对象类	LDAP 组对象类 （通常是 groupofNames）。
	组成员资格属性	代表用户组成员资格的属性。不要在该名称中使用空格。
	使用动态组	如果需要使用动态组，请选择该选项。
	动态组对象类	LDAP 动态组对象类 （一般 dynamicGroup）。
eDirectory 证书	*密钥存储区路径*	必需。指定应用程序服务器用于运行的、 JRE 的密钥存储区 (cacerts) 文件的完整路径，或单击小浏览器按钮，然后浏览找到 cacerts 文件。 User Application 安装过程中将修改密钥存储区文件。在 Linux 或 Solaris 上，用户必须具有写此文件的权限。
	密钥存储区口令	必需。指定 cacerts 口令。默认值为 changeit。
	确认密钥存储区口令	
私用密钥存储区	*私用密钥存储区路径*	私用密钥存储区包含 User Application 的私用密钥和证书。保留 . 如果保留为空的话，将采用默认路径 /jre/lib/security/cacerts。
	私用密钥存储区口令	口令为 changeit，除非另行指定。此口令已使用主密钥进行过加密。
	私用密钥别名	别名为 novellIDMUserApp，除非另行指定。
	私用密钥口令	口令为 novellIDM，除非另行指定。此口令已使用主密钥进行过加密。

设置类型	字段	说明
可信密钥存储区	*可信存储区路径*	可信密钥存储区包含所有用于验证数字签名的可信签名者的证书。如果此路径为空的话，User Application 将从系统属性 javax.net.ssl.trustStore 中获取路径。如果那里没有路径，则假定为 jre/lib/security/cacerts。
	可信存储口令	如果此字段为空的话，User Application 将从系统属性 javax.net.ssl.trustStorePassword 中获取口令。如果那里没有值，则使用 changeit。此口令已使用主密钥进行过加密。
Novell Audit 数字签名和证书密钥		包容 Novell Audit 数字签名密钥和证书。
	Novell Audit 数字签名证书	显示数字签名证书。
	Novell Audit 数字签名私用密钥	显示数字签名私用密钥。此密钥已使用主密钥进行过加密。
iChain 设置	*已启用 ICS 注销*	如果选中了此选项，则 User Application 支持同时注销 User Application 和 iChain 或 Novell Access Manager。注销时，User Application 检查是否存在 iChain 或 Novell Access Manager Cookie，如果存在 Cookie，则将用户重路由到 ICS 注销页。
	ICS 注销页	iChain 或 Novell Access Manager 注销页的 URL，其中该 URL 是 iChain 或 Novell Access Manager 预期的主机名。如果启用了 ICS 日志记录并且用户要注销 User Application，则将用户重路由到此页面。

设置类型	字段	说明
电子邮件	*通知模板 HOST 令牌*	指定主管 Identity Manager User Application 的应用程序服务器。例如： `myapplication serverServer` 此值将替换电子邮件模板中的 $HOST$ 令牌。所建立的 URL 是指向供应请求任务和批准通知的链接。
	通知模板 PORT 令牌	用于替换供应请求任务和批准通知所用的电子邮件模板中的 $PORT$ 令牌。
	通知模板 SECURE PORT 令牌	用于替换供应请求任务和批准通知所用的电子邮件模板中的 $SECURE_PORT$ 令牌。
	通知模板 PROTOCOL 令牌	指非安全协议 HTTP。用于替换供应请求任务和批准通知所用的电子邮件模板中的 $PROTOCOL$ 令牌。
	通知模板 SECURE PROTOCOL 令牌	指安全协议 HTTPS。用于替换供应请求任务和批准通知所使用电子邮件模板中的 $SECURE_PROTOCOL$ 令牌。
	通知 SMTP 电子邮件发件人：	指定供应电子邮件中发送电子邮件的用户。
	通知 SMTP 电子邮件主机：	指定供应电子邮件所使用的 SMTP 电子邮件主机。这可以是 IP 地址或 DNS 名。
口令管理		
	使用外部口令 WAR	通过此功能，可以指定外部忘记口令 WAR 中的“忘记口令”页，或外部忘记口令 WAR 用于通过万维网服务回拨 User Application 的 URL。 如果选择*使用外部口令 WAR*，则必须提供*忘记口令链接*和*忘记口令返回链接*的值。 如果没有选择*使用外部口令 IDM*，则 IDM 将使用默认的内部口令管理功能。 /jsps/pwdmgt/ForgotPassword.jsf （开头没有 http(s) 协议）。这将用户重定向到内置于 User Application 的 “忘记口令”功能，而不是外部 WAR。
	忘记口令链接	此 URL 指向 “忘记口令”功能页。指定外部或内部口令管理 WAR 中的 ForgotPassword.jsf 文件。
	忘记口令返回链接	如果使用的是外部口令管理 WAR，需提供外部口令管理 WAR 用来通过万维网服务回调 User Application 的路径，例如 https://*idmhost:sslport*/idm。

设置类型	字段	说明
杂项	*会话超时*	应用程序会话超时。
	OCSP URI	如果客户安装使用在线证书状态协议 (OCSP)，请提供统一资源标识符 (URI)。例如，格式为 http://host:port/ocspLocal。 OCSP URI 在线更新可信证书的状态。
	授权配置路径	授权配置文件的完全限定名。
	创建 eDirectory 索引	
	服务器 DN	
树枝对象	*所选*	选择要使用的每个数字对象类型。
	树枝对象类型	有以下标准树枝可供选择：位置、国家 / 地区、组织单位、组织和域。也可以在 iManager 中自己定义树枝，然后在*添加新树枝对象*下面添加这些树枝。
	树枝属性名称	列出与树枝对象类型相关的属性类型名称。
	添加新的树枝对象：树枝对象类型	指定可作为树枝的身份库 中的对象类的 LDAP 名称。 有关树枝的信息，请参见 《*Novell iManager 2.6 管理指南 (http://www.novell.com/documentation/imanager26/pdfdoc/imanager_admin_26/imanager_admin_26.pdf)*》。
	添加新的树枝对象：树枝属性名称	提供树枝对象的属性名称。

4 完成设置配置之后，单击*确定*，然后继续第 5.6.10 节 “校验选择并安装”（第 154 页）。

5.6.10 校验选择并安装

1 阅读 “安装前摘要”页，校验所选择的安装参数。

2 如有必要，使用*后退*返回到前面的安装页，对安装参数作出更改。

User Application 配置页的值没有保存下来，因此，在重新指定安装中的以前页面之后，必须重新输入 User Application 配置值。

3 当安装和配置参数满意之后，返回 “安装前摘要”页，然后单击*安装*。继续第 5.6.11 节 “查看日志文件”（第 155 页）。



5.6.11 查看日志文件

如果安装成功完成，没有错误，请继续第 5.6.12 节 “添加 User Application 配置文件和 JVM 系统属性”（第 155 页）。

如果安装提示出现错误或警告，请检查日志文件以确定问题：

- Identity_Manager_User_Application_Installlog.log 保存基本安装任务的结果。
- Novell-Custom-Install.log 记录了有关安装过程中所执行的 User Application 配置。

5.6.12 添加 User Application 配置文件和 JVM 系统属性

1 将 sys-configuration-xmldata.xml 文件从 User Application 安装目录复制到主管 WebSphere 服务器的计算机上的某个目录，例如， /UserAppConfigFiles。 User Application 安装目录是安装有 User Application 的目录。

2 在 JVM 系统属性中设置 sys-configuration-xmldata.xml 文件的路径。作为管理员用户登录到 WebSphere 管理控制台执行此操作。

3 从左面板中，转到*服务器 > 应用程序服务器*。

4 单击服务器列表中的服务器名称，例如 server1。

5 在右边的设置列表中，转到*服务器基础结构*下的 *Java 和进程管理*。

6 展开链接，并选择*进程定义*。

7 在*其他属性*列表下，选择 *Java 虚拟机*。

8 选择 JVM 页标题*其他属性*下的*自定义属性*。

9 单击*新建*可添加新 JVM 系统属性。

9a 对于*名称*，指定 extend.local.config.dir。

9b 对于*值*，指定复制了 sys-configuration-xmldata.xml 文件的目录，例如，/UserAppConfigFiles。

9c 对于*说明*，指定属性的说明，例如 sys-configuration-xmldata.xml 的路径。

9d 单击*确定*以保存属性。

10 单击*新建*可添加其他新 JVM 系统属性。

10a 对于*名称*，指定 idmuserapp.logging.config.dir

10b 对于*值*，指定复制了 sys-configuration-xmldata.xml 文件的目录，例如，/UserAppConfigFiles。

10c 对于*说明*，指定属性的说明，例如 sys-configuration-xmldata.xml 的路径。

10d 单击*确定*以保存属性。

注释 : idmuserapp-logging.xml 文件不需要存在于此目录中。它在进行日志记录配置更改时创建。

---

11 继续下一部分第 5.6.13 节 "将 eDirectory 可信根导入 WebSphere 密钥存储区"（第 156 页）。

5.6.13 将 eDirectory 可信根导入 WebSphere 密钥存储区

1 User Application 安装过程将 eDirectory 可信根证书导出到安装 User Application 的目录。将这两个证书复制到主管 WebSphere 服务器的计算机。

2 将证书导入到 WebSphere 密钥存储区中。可以使用 WebSphere 管理员控制台 (通过 WebSphere 管理员控制台导入证书 （第 156 页）) 或通过命令行 (通过命令行导入证书 （第 156 页）) 执行此操作。

3 导入证书后，继续执行第 5.6.14 节 "部署 IDM WAR 文件"（第 157 页）。

通过 WebSphere 管理员控制台导入证书

1 作为管理员用户登录到 WebSphere 管理控制台。

2 从左面板中，转到*安全性 > SSL 证书和密钥管理*。

3 在右侧的设置列表中，转到*其他属性*下的*密钥存储区和证书*。

4 选择*节点默认信任存储区*（或正在使用的信任存储区）。

5 在右侧的*其他属性*下，选择*签名者证书*。

6 单击*添加*。

7 键入别名和证书文件的完整路径。

8 在下拉菜单中将 "数据" 类型更改为*二进制 DER 数据*。

9 单击*确定*。现在，应该在签名者证书列表中看到证书。

通过命令行导入证书

1 在主管 WebSphere 服务器的计算机上，通过命令行运行密钥工具，将证书导入到 WebSphere 密钥存储区中。

注释 : 需要使用 WebSphere 密钥工具，否则此操作不起作用。此外，应确保存储区类型为 PKCS12。

WebSphere 密钥工具位于 /IBM/WebSphere/AppServer/java/bin。

示例密钥工具命令

keytool -import -trustcacerts -file servercert.der -alias myserveralias -keystore trust.p12 -storetype PKCS12

如果系统中有多个 trust.p12 文件，则可能需要指定该文件的完整路径。

5.6.14 部署 IDM WAR 文件

1. 作为管理员用户登录到 WebSphere 管理控制台。
2. 从左面板中，转到*应用程序 > 安装新应用程序*
3. 浏览到 IDM War 文件的位置。(IDM WAR 文件在安装 User Application 过程中配置。该文件位于您在安装 User Application 过程中指定的 User Application 安装目录。)
4. 在 "环境" 中键入应用程序的根，例如 IDMProv。这将是 URL 路径。
5. 请确保选中了*仅当需要其他信息时提示我*，然后单击*下一步*，转到*选择安装选项*页。
6. 接受此页的默认值，然后单击*下一步*，转到*将模块映射到服务器*屏幕。
7. 将此页的所有设置保留默认值，然后单击*下一步*，转到*将资源参照映射到资源*页。
8. 对于鉴定方法，选中*用户默认方法*复选框。然后，在*鉴定数据项*下拉列表中，选择先前创建的别名，例如 MyServerNode01/MyAlias。
9. 在鉴定设置下方的表中，找到要部署的模块。在标题为目标资源 JNDI 名称的列下，单击浏览按钮指定一个 JNDI 名称。将显示一个资源列表。选择先前创建的数据源，然后单击*应用*按钮返回到将资源参照映射到资源页，(例如， MyDataSource)。
10. 选择*下一步*，转到*映射万维网模块的虚拟主机*页。
11. 将此页的所有设置保留默认值，然后单击*下一步*，转到*摘要*页。
12. 单击*完成*以完成部署。
13. 部署完成后，单击*保存*以保存更改。
14. 继续第 5.6.15 节 "启动应用程序" (第 157 页)。

5.6.15 启动应用程序

1. 作为管理员用户登录到 WebSphere 管理员控制台。
2. 在左侧的导航面板中，转到*应用程序 > 企业应用程序*。
3. 选中要启动的应用程序旁的复选框，然后单击*启动*。

   启动后，*应用程序状态*列将显示一个绿色箭头。

5.6.16 访问 User Application 门户

1. 使用在部署过程中指定的环境访问门户。

在 WebSphere 上，万维网容器的默认端口是 9080，安全端口是 9443。 URL 的格式为：

http:// <*server*>:9080/IDMProv

5.7 从控制台界面安装 User Application

本部分说明如何通过使用安装程序的控制台 （命令行）版本安装 Identity Manager User Application。

1 获取表 5-2 （第 104 页）中说明的相应安装文件。

2 登录并打开终端会话。

3 使用以下命令，通过 Java 起动平台的安装程序：

   java -jar IdmUserApp.jar -i console

4 在导入步骤或创建主密钥步骤中，按照第 5.5 节 “在 JBoss 应用程序服务器上从安装 GUI 安装 User Application”（第 105 页）中针对图形用户界面说明的相同步骤，阅读命令行上的提示符并在命令行上输入相应的回复。

5 要设置 User Application 配置参数，必须手动启动 configupdate 实用程序。在命令行上，输入 Configupdate.sh （Linux 或 solaris）或 Configupdate.bat (windows)，然后输入如第 5.5.14 节 “配置 User Application”（第 121 页）中所述的值。

6 如果使用的是外部口令管理 WAR，请手动将其复制到安装目录和运行外部口令 WAR 功能的远程 JBoss 服务器部署目录。

7 继续第 5.9 节 “安装后的任务”（第 163 页）。

5.8 使用单个命令安装 User Application

本部分说明如何执行静默安装。对于静默安装，在安装过程中无需交互操作，从而可以节省您的时间，尤其在多个系统上执行安装时。 Linux 和 Solaris 上的程序安装支持静默方式。

1 获取表 5-2 （第 104 页）中列出的相应安装文件。

2 登录并打开终端会话。

3 找到安装文件中附带的 IDM 属性文件 silent.properties。如果使用 CD，请将此文件复制到本地。

4 编辑 silent.properties 以提供安装参数和 User Application 配置参数。

   有关每个安装参数的示例，请参见 silent.properties 文件。安装参数与在 GUI 或控制台安装过程中设置的安装参数对应。

   有关每个 User Application 配置参数的说明，请参见表 5-8。User Application 配置参数和在 GUI 或控制台安装步骤或使用 configupdate 实用程序所设置的参数一致。

5 使用以下命令起动静默安装：

   java -jar IdmUserApp.jar -i silent -f / *您的目录路径* /silent.properties

   如果文件所在目录不同于安装程序底稿中的目录，请键入 silent.properties 的完整路径。此底稿将必要文件释放到临时目录并启动静默安装。

表 5-8 静默安装的 User Application 配置参数

silent.properties 中的 User Application 参数名称	User Application 配置参数文件中的等价参数名及说明
NOVL_CONFIG_LDAPHOST=	eDirectory 连接设置：LDAP 主机。必需。为 LDAP 服务器指定主机名或 IP 地址。
NOVL_CONFIG_LDAPADMIN=	必需。指定 LDAP 管理员的身份凭证。该用户必须已经存在。User Application 使用此帐户来建立与身份库 的管理连接。此值已使用主密钥进行过加密。
NOVL_CONFIG_LDAPADMINPASS=	eDirectory 连接设置：LDAP 管理员口令。必需。指定 LDAP 管理员口令。此口令已使用主密钥进行过加密。
NOVL_CONFIG_ROOTCONTAINERNAME=	eDirectory DN：根树枝 DN。必需。指定根树枝的 LDAP 判别名。如果没有在目录抽象层中指定搜索根，则将该判别名用作默认的实体定义搜索根。
NOVL_CONFIG_PROVISIONROOT=	eDirectory DN：供应驱动程序 DN。必需。指定以前在第 5.3 节 "创建 User Application 驱动程序"（第 100 页）中创建的 User Application 驱动程序的判别名。例如，如果驱动程序为 UserApplicationDriver，驱动程序集称为 myDriverSet，并且驱动程序集位于环境 o=myCompany 中，则可以输入以下值： `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
NOVL_CONFIG_LOCKSMITH=	eDirectory DN：User Application Admin。必需。身份库 中有权执行所指定 User Application 用户树枝的管理任务的现有用户。该用户可以使用 User Application 的*管理*选项卡管理入口。 如果 User Application 管理员参与 iManager、Designer for Identity Manager 或 User Application（*请求和批准*选项卡）中显示的工作流程管理任务，则必须授予此管理员对 User Application 驱动程序中包含的对象实例的相应受托者权限。有关细节，请参见 《*IDM User Application：管理指南*》。 要在部署 User Application 之后更改指派，必须使用 User Application 中的*管理* > *安全*页面。
NOVL_CONFIG_PROVLOCKSMITH=	eDirectory DN：供应应用程序 Admin。 Identity Manager 3.5.1 的供应版本中可以使用此角色。供应应用程序管理员使用*供应***选项卡** （*管理*选项卡下方）来管理供应工作流程功能。用户可以通过 User Application 的*请求和批准*选项卡使用这些功能。在将用户指定为供应应用程序管理员之前，身份库 中必须存在此用户。 要在部署 User Application 之后更改指派，必须使用 User Application 中的*管理* > *安全*页面。

silent.properties 中的 User Application 参数名称	User Application 配置参数文件中的等价参数名及说明
NOVL_CONFIG_USERCONTAINERDN=	元目录用户身份：用户树枝 DN。必需。指定用户树枝的 LDAP 判别名 (DN) 或完全限定的 LDAP 名称。这定义用户和组的搜索范围。允许该树枝中（及其下）的用户登录 User Application。 **重要：** 如果要使该用户能够执行工作流程，请确保在 User Application 驱动程序设置过程中指定的 User Application 管理员在该树枝中存在。
NOVL_CONFIG_GROUPCONTAINERDN=	元目录用户组：组树枝 DN。必需。指定组树枝的 LDAP 判别名 (DN) 或完全限定的 LDAP 名称。由目录抽象层中的实体定义使用。
NOVL_CONFIG_KEYSTOREPATH=	eDirectory 证书：密钥存储区路径。必需。指定应用程序服务器所使用的 JRE 的密钥存储区 (cacerts) 文件。User Application 安装过程中将修改密钥存储区文件。在 Linux 或 Solaris 上，用户必须具有写此文件的权限。
NOVL_CONFIG_KEYSTOREPASSWORD=	eDirectory 证书：密钥存储区口令。必需。指定 cacerts 口令。默认值为 changeit。
NOVL_CONFIG_SECUREADMINCONNECTION=	eDirectory 连接设置：安全 Admin 连接。 通过指定为 True，可以要求所有使用 admin 帐户的通讯都通过安全套接字进行 （不选中此选项则相反）。 如果 Admin 帐户不使用安全套接字通讯，则指定为 Faulse。
NOVL_CONFIG_SECUREUSERCONNECTION=	eDirectory 连接设置：安全用户连接。 通过指定为 True，可以要求所有使用已登录用户帐户的通讯都通过安全套接字进行 （不选中此选项则相反）。 如果用户的帐户不使用安全套接字通讯，则指定为 False。
NOVL_CONFIG_SESSIONTIMEOUT=	杂项：会话超时。指定应用程序会话超时时间间隔。
NOVL_CONFIG_LDAPPLAINPORT=	eDirectory 连接设置：LDAP 非安全端口。为 LDAP 服务器指定非安全端口，比如 389。
NOVL_CONFIG_LDAPSECUREPORT=	eDirectory 连接设置：LDAP 安全端口。为 LDAP 服务器指定安全端口，比如 636。
NOVL_CONFIG_ANONYMOUS=	eDirectory 连接设置：使用公开匿名帐户。 指定为 Ture 可以允许没有登录的用户访问 LDAP 公开匿名帐户。 指定 False 转为启用 NOVL_CONFIG_GUEST 。

silent.properties 中的 User Application 参数名称	User Application 配置参数文件中的等价参数名及说明
NOVL_CONFIG_GUEST=	eDIRECTORY 连接设置：LDAP Guest。允许没有登录的用户访问允许的入口小程序。同时必须取消选择*使用公开匿名帐户*。身份库 中必须已经存在 Guest 用户帐户。要禁用 Guest 用户，请选择*使用公开匿名帐户*。
NOVL_CONFIG_GUESTPASS=	eDIRECTORY 连接设置：LDAP Guest 口令。
NOVL_CONFIG_EMAILNOTIFYHOST=	电子邮件：通知模板 HOST 令牌。指定主管 Identity Manager User Application 的应用程序服务器。例如： `myapplication serverServer` 此值将替换电子邮件模板中的 $HOST$ 令牌。所建立的 URL 是指向供应请求任务和批准通知的链接。
NOVL_CONFIG_EMAILNOTIFYPORT=	电子邮件：通知模板 Port 令牌。用于替换供应请求任务和批准通知所用的电子邮件模板中的 $PORT$ 令牌。
NOVL_CONFIG_EMAILNOTIFYSECUREPORT=	电子邮件：通知模板 Secure Port 令牌。用于替换供应请求任务和批准通知所使用电子邮件模板中的 $SECURE_PORT$ 令牌。
NOVL_CONFIG_NOTFSMTPEMAILFROM=	电子邮件：通知 SMTP 电子邮件发件人。指定供应电子邮件中发送电子邮件的用户。
NOVL_CONFIG_NOTFSMTPEMAILHOST=	电子邮件：通知 SMTP 电子邮件主机。指定供应电子邮件所使用的 smtp 电子邮件主机。这可以是 IP 地址或 DNS 名。
NOVL_CONFIG_USEEXTPWDWAR=	口令管理：使用外部口令 WAR。 如果使用外部口令管理 WAR，指定为 True。如果指定为 True，还必须提供 *NOVL_CONFIG_EXTPWDWARPTH* 和 *NOVL_CONFIG_EXTPWDWARRTNPATH* 的值。 指定为 False 可以使用默认的外部口令管理功能。 /jsps/pwdmgt/ForgotPassword.jsf （开头没有 http(s) 协议）。这将用户重定向到内置于 User Application 的 “忘记口令”功能，而不是外部 WAR。
NOVL_CONFIG_EXTPWDWARPATH=	口令管理：忘记口令链接。指定外部或内部口令管理 WAR 中的 “忘记口令”功能页的 URL ForgotPassword.jsf。或者接受默认的内部口令管理 WAR。有关细节，请参见 使用口令 WAR （第 131 页）。
NOVL_CONFIG_EXTPWDWARRTNPATH=	口令管理：忘记口令返回链接。如果使用的是外部口令管理 WAR，需提供外部口令管理 WAR 用来通过万维网服务回调 User Application 的路径，例如 https:// *idmhost:sslport*/idm。
NOVL_CONFIG_USEROBJECTATTRIBUTE=	元目录用户身份：用户对象类。 LDAP 用户对象类（通常为 inetOrgPerson）。

silent.properties 中的 User Application 参数名称	User Application 配置参数文件中的等价参数名及说明
NOVL_CONFIG_LOGINATTRIBUTE=	元目录用户身份：登录属性。代表用户的登录名的 LDAP 属性 （比如 CN）。
NOVL_CONFIG_NAMINGATTRIBUTE=	元目录用户身份：命名属性。用作查找用户或组时的标识符的 LDAP 属性。这不同于登录属性，登录属性仅在登录时使用，在用户 / 组搜索时不使用。
NOVL_CONFIG_USERMEMBERSHIPATTRIBUTE=	元目录用户身份：用户成员资格属性。可选。代表用户的组成员资格的 LDAP 属性。不要在该名称中使用空格。
NOVL_CONFIG_GROUPOBJECTATTRIBUTE=	元目录用户组：组对象类。 LDAP 组对象类 （通常是 groupofNames）。
NOVL_CONFIG_GROUPMEMBERSHIPATTRIBUTE=	元目录用户组：组成员资格属性。指定代表用户组成员资格的属性。不要在该名称中使用空格。
NOVL_CONFIG_USEDYNAMICGROUPS=	元目录用户组：使用动态组。要使用动态组，指定为 True。否则，指定为 False。
NOVL_CONFIG_DYNAMICGROUPOBJECTCLASS=	元目录用户组：动态组对象类。指定 LDAP 动态组对象类 （一般为 dynamicGroup）。
NOVL_CONFIG_PRIVATESTOREPATH=	私用密钥存储区：私用密钥存储区路径。指定包含 User Application 的私用密钥和证书的私用密钥存储区的路径。保留 . 如果保留为空的话，将采用默认路径 /jre/lib/security/cacerts。
NOVL_CONFIG_PRIVATESTOREPASSWORD=	私用密钥存储区：私用密钥存储区口令。
NOVL_CONFIG_PRIVATEKEYALIAS=	私用密钥存储区：私用密钥别名。别名为 novellIDMUserApp，除非另行指定。
NOVL_CONFIG_PRIVATEKEYPASSWORD=	私用密钥存储区：私用密钥口令。
NOVL_CONFIG_TRUSTEDSTOREPATH=	可信密钥存储区：可信存储路径。可信密钥存储区包含所有用于验证数字签名的可信签名者的证书。如果此路径为空的话，User Application 将从系统属性 javax.net.ssl.trustStore 中获取路径。如果那里没有路径，则假定为 jre/lib/security/cacerts。
NOVL_CONFIG_TRUSTEDSTOREPASSWORD=	可信密钥存储区：可信存储口令。
NOVL_CONFIG_AUDITCERT=	Novell Audit 数字签名证书。
NOVL_CONFIG_AUDITKEYFILEPATH=	Novell Audit 数字签名私用密钥文件路径。
NOVL_CONFIG_ICSLOGOUTENABLED=	iChain 设置：启用 ICS 注销。 通过指定为 True，可以启用同时注销 User Application 和 iChain 或 Novell Access Manager。注销时，User Application 检查是否存在 iChain 或 Novell Access Manager Cookie，如果存在 Cookie，则将用户重路由到 ICS 注销页。 通过指定为 False，可以禁用同时注销。

silent.properties 中的 User Application 参数名称	User Application 配置参数文件中的等价参数名及说明
NOVL_CONFIG_ICSLOGOUTPAGE=	iChain 设置：ICS 注销页。指定 iChain 或 Novell Access Manager 注销页的 URL，其中该 URL 是 ICHAIN 或 Novell Access Manager 预期的主机名。如果启用了 ICS 日志记录并且用户要注销 User Application，则将用户重路由到此页面。
NOVL_CONFIG_EMAILNOTIFYPROTOCOL=	电子邮件：通知模板 PROTOCOL 令牌。指非安全协议 HTTP。用于替换供应请求任务和批准通知所用的电子邮件模板中的 $PROTOCOL$ 令牌。
NOVL_CONFIG_EMAILNOTIFYSECUREPROTOCOL=	电子邮件：通知模板 Secure Port 令牌。
NOVL_CONFIG_OCSPURI=	杂项：OCSP URL。如果客户安装使用在线证书状态协议 (OCSP)，请提供统一资源标识符 (URI)。比如，格式为 http://host:port/ocsplocal。OCSP URI 在线更新可信证书的状态。
NOVL_CONFIG_AUTHCONFIGPATH=	杂项：授权配置路径。授权配置文件的完全限定名。

5.9 安装后的任务

安装并配置 User Application 之后，需执行安装后的任务。

- 第 5.9.1 节 “记录主密钥”（第 163 页）
- 第 5.9.2 节 “检查群集安装”（第 164 页）
- 第 5.9.3 节 “配置 JBoss 服务器之间的 SSL 通讯”（第 164 页）
- 第 5.9.4 节 “访问外部口令 WAR”（第 164 页）
- 第 5.9.5 节 “升级忘记口令设置”（第 165 页）
- 第 5.9.6 节 “设置电子邮件通知”（第 165 页）
- 第 5.9.7 节 “在 JBoss 应用程序服务器上测试安装”（第 165 页）
- 第 5.9.8 节 “设置供应小组和请求”（第 166 页）
- 第 5.9.9 节 “在 eDirectory 中创建索引”（第 166 页）

5.9.1 记录主密钥

在安装后，立即复制加密的主密钥并将其记录在一个安全的位置。

1 打开安装目录中的 master-key.txt 文件。

2 将经过加密的主密钥复制到一个安全位置，保证系统故障时也能访问。

警告：要始终保留加密主密钥的复本。如果丢失了主密钥，比如由于设备发生故障，则需要使用经过加密的主密钥重获加密数据的访问权。

如果此安装位于群集的第一个成员上，当在群集中其他成员上安装 User Application 驱动时，需使用此经加密的主密钥。

有关主密钥的更多信息，请参见 《*Identity Manager User Application：管理指南* (http://www.novell.com/documentation/idm35/index.html)》中的*重要 User Application 数据的加密*和*群集 JBoss* 部分。

5.9.2 检查群集安装

检查群集安装。请确保 JBoss 群集中的每个 JBoss 服务器都具有以下设置：

- 唯一分区名 （分区名称）
- 唯一分区 UDP （partition.udpGroup）
- 唯一工作流程引擎 ID
- 同一 WAR 文件。安装过程中，默认情况下， WAR 被写到 jboss\server\IDM\deploy 目录。

请确保 WebSphere 群集中的每个服务器都具有唯一的工作流程引擎 ID。

有关详细信息，请参见 《*Identity Manager User Application：管理指南* (http://www.novell.com/documentation/idm35/index.html)》第 4 章中关于 “群集”的部分。

5.9.3 配置 JBoss 服务器之间的 SSL 通讯

如果安装过程中在 User Application 配置文件中选择了*使用外部口令 WAR*，则必须配置部署 User Application WAR 和 IDMPwdMgt.war 文件的 JBoss 服务器之间的 SSL 通讯。有关指导，请参见 JBoss 文档。

5.9.4 访问外部口令 WAR

如果有外部口令 WAR 并且想试验一下 “忘记口令”功能，则可以从两个位置访问该功能：

- 在浏览器中。转至外部口令 WAR 中的 “忘记口令”页，比如 http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf。
- 在 “User Application 登录”页上，单击*忘记口令*链接。

5.9.5 升级忘记口令设置

可以在安装后更改*忘记口令链接*和*忘记口令返回链接*的值。或者使用 configupdate 实用程序，或者使用 User Application。

要使用 configupdate 实用程序：在命令行上，将目录更改为安装目录，然后输入 configupdate.sh （linux 或 Solaris）或 configupdate.bat (Windows)。如果要创建或编辑外部口令管理 WAR，那么，在将 WAR 复制到远程 JBoss 服务器之前，必须手动重命名 WAR。

要使用 User Application：以 User Application 管理员身份登录，然后转至*管理 > 应用程序配置 > 口令模块设置 > 登录*。修改以下字段：

- *忘记口令链接*（例如：http://localhost:8080/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsf）
- *忘记口令返回链接*（例如：https://idmhost:sslport/idm）

5.9.6 设置电子邮件通知

要实施 “忘记口令” 和 “工作流程电子邮件通知” 功能：

1 在 iManager 中，在 “角色和任务” 下面，选择*工作流程管理*，然后选择*电子邮件服务器选项*。

2 在*主机名*下面指定 SMTP 服务器的名称。

3 在*收件人*旁边，指定一个电子邮件地址 （比如 *noreply@novell.com*），然后单击*确定*。

5.9.7 在 JBoss 应用程序服务器上测试安装

1 启动数据库。有关指导，请参见数据库文档。

2 启动 User Application 服务器 (JBoss) 在命令行上，将安装目录更改为工作目录，然后执行以下底稿 （由 User Application 安装所提供）：

start-jboss.sh （Linux 和 Solaris）

start-jboss.bat (Windows)

如果需要停止应用程序服务器，请使用 stop-jboss.sh 或 stop-jboss.bat，或关闭 start-jboss.sh 或 start-jboss.bat 正在运行的窗口。

3 启动 User Application 驱动程序。这将启动到 User Application 驱动程序的通讯。

3a 登录 iManager。

3b 在左侧浏览帧中显示的 “角色和任务” 中，选中 *Identity Manager* 下面的 *Identity Manager 概述*。

3c 在显示的内容视图中，指定包含 User Application 驱动程序的驱动程序集，然后单击*搜索*。将出现一个图形，其中显示该驱动程序集及其关联的驱动程序。

3d 单击驱动程序上的红白色图标。

3e 选择*启动驱动程序*。驱动程序状态更改为阴阳符号，指示驱动程序先已启动。

在启动时，驱动程序将尝试与 User Application 进行 “握手” 通讯。如果应用程序服务器没有运行，或者如果 WAR 未成功部署，则驱动程序将返回错误。

4 要启动并登录到 User Application，请使用万维网浏览器并访问以下 URL：

http:// *hostname*: *port*/ *ApplicationName*

其中 *hostname*: *port* 是应用程序服务器主机名 （比如 myserver.domain.com），而 port 为应用程序服务器的端口 （比如， JBoss 上默认采用 8080）。默认情况下，*ApplicationName* 为 IDM。应用程序名称在安装过程中提供应用程序服务器配置信息时指定。

会显示 Novell Identity Manager User Application 主页。

5 在该页的右上角，单击*登录*可登录 User Application。

完成这些步骤之后，如果浏览器中还没有显示 Identity Manager User Application 页，请检查终端控制台上是否有错误讯息，并参见第 5.11 节 “查错”（第 167 页）。

5.9.8 设置供应小组和请求

设置供应小组和供应小组请求以启用工作流程任务。有关指导，请参见 《*Identity Manager 3.5.1 User Application：管理指南* (http://www.novell.com/documentation/idm35/index.html)》。

5.9.9 在 eDirectory 中创建索引

为改进 IDM User Application 的性能， eDirectory 管理员必须创建 manager、 ismanager 和 srvprvUUID 属性的索引。如果没有这些属性的索引，User Application 用户可能会遇到不良性能，尤其在群集环境中。有关使用索引管理器创建索引的指导，请参见 《*Novell eDirectory 管理指南*》(http://www.novell.com/documentation)。

5.10 安装后重新配置 IDM WAR 文件。

1 通过执行 configupdate.sh 或 configupdate.bat，运行 User Application 安装目录中的 ConfigUpdate 实用程序。这使您能够更新安装目录中的 WAR 文件。

   有关 ConfigUpdate 实用程序参数的信息，请参见第 5.5.14 节 “配置 User Application”（第 121 页）或第 5.6.9 节 “配置 User Application”（第 144 页）。

2 将新 WAR 文件部署到应用程序服务器。

5.11 查错

Novell 代表将会帮您解决遇到的任何安装和配置问题。同时，这里提供了一些在您遇到某些问题时可以尝试的操作。

表 5-9 User Application 查错

问题	建议的操作

想要修改在安装过程中设置的 User Application 配置。这包括类似于下列项目的配置：
◆ 身份库 连接和证书
◆ 电子邮件设置
◆ 元目录用户身份、用户组
◆ iChain 设置
	可以运行配置实用程序，而不论是否运行了安装程序。
	在 Linux 和 Solaris 上，从安装目录 （默认为 /opt/novell/idm）运行以下命令：
	`configupdate.sh`
	在 Windows 上，从安装目录 （默认为 c:\opt\novell\idm）运行以下命令：
	`configupdate.bat`

应用程序服务器启动时出现异常，显示日志讯息端口 8080 已被使用。	关闭 Tomcat （或其他服务器软件）的可能已在运行的任何实例。如果决定将应用程序服务器重新配置为使用 8080 以外的其他端口，请记住在 iManager 中编辑 User Application 驱动程序的配置设置。
当应用程序服务器启动时，显示讯息称找不到任何可信证书。	确保使用在 User Application 安装中所指定的 JDK 启动应用程序服务器。
无法登录门户 Admin 页。	确保存在 User Application 管理员帐户。不要将此帐户与 iManager Admin 帐户相混淆。存在着 （或应该有）两个不同的 Admin 对象。
可以以 Admin 身份登录，但不能创建新用户。	User Application 管理员必须是顶层树枝的受托者，并且需要有主管权限。作为权宜之计，可以尝试将 User Application 管理员的权限设置为等效于 LDAP 管理员的权限 （使用 iManager）。

问题	建议的操作
当启动应用程序服务器时，出现 MySQL 连接错误。	请不要以 root 身份运行。（然而，如果您运行随 IDM 提供的 MySQL 版本时，几乎不会出现此问题。） 确保 MySQL 正在运行 （并且适当的拷贝正在运行）。停止 MySQL 的其他任何实例。运行 /idm/mysql/start-mysql.sh，然后运行 /idm/start-jboss.sh。 在文本编辑器中检查 /idm/mysql/setup-mysql.sh，并纠正任何可疑的值。然后运行底稿，再运行 /idm/start-jboss.sh。
启动 应用程序服务器时遇到密钥存储区错误 .	应用程序服务器没有运行在安装 User Application 时所指定的 JDK。 使用 keytool 命令导入证书文件： `keytool -import -trustcacerts -alias aliasName -file certFile -keystore ..\lib\security\cacerts -storepass changeit` ◆ 使用为该证书选择的唯一名称替换 *aliasName*。 ◆ 使用证书文件的完整路径和名称替换 *certFile*。 ◆ 默认的密钥存储区口令为 changeit （如果有其他口令，请指定）。

没有发送电子邮件通知。	运行 configupdate 实用程序检查是否提供了 “电子邮件发件人” 和 “电子邮件主机 User Application” 配置参数的值。
	
	在 Linux 或 Solaris 上，从安装目录 （默认为 /opt/novell/idm）运行以下命令：
	
	`configupdate.sh`
	
	在 Windows 上，从安装目录 （默认为 c:\opt\novell\idm）运行以下命令：
	
	`configupdate.bat`

激活 Novell Identity Manager 产品 6

以下信息说明激活如何影响基于 Novell® Identity Manager 的产品。Identity Manager、集成模块和供应模块都必须在安装后 90 天内进行激活，否则它们将会关闭。可以在这 90 天期限内的任何时间，或者此后的任何时间，选择激活 Identity Manager 产品。

可以通过完成以下任务激活 Identity Manager 和驱动程序：

- 购买 Identity Manager 产品许可证
- 通过使用身份凭证激活 Identity Manager 产品
- 安装产品激活身份凭证
- 查看 Identity Manager 和驱动程序的产品激活

6.1 购买 Identity Manager 产品许可证

要购买 Identity Manager 产品许可证，请参见 Novell Identity Manager “如何购买”万维网网页 (http://www.novell.com/products/identitymanager//howtobuy.html)

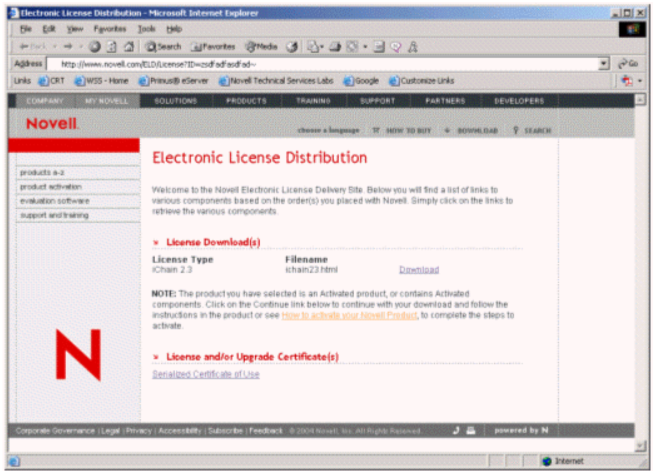
在您购买产品许可证后， Novell 将通过电子邮件向您发送一个客户 ID。该电子邮件还包含 Novell 站点的 URL，您可以从该站点获取身份凭证。如果您记不起或者没有收到客户 ID，美国内请拨打 1-800-418-8373 联系 “Novell 激活中心”，对于其他所有地方，请拨打 1-801-861-8373。（使用 801 区域代码拨打会收取费用。）

6.2 通过使用身份凭证激活 Identity Manager 产品

1 在您购买许可证之后， Novell 会向您发送一封电子邮件，其中包含您的客户 ID。在该电子邮件的 “订单细节”部分下方，还包含一个链接，指向可获得您的身份凭证的站点。单击该链接可转至该站点。

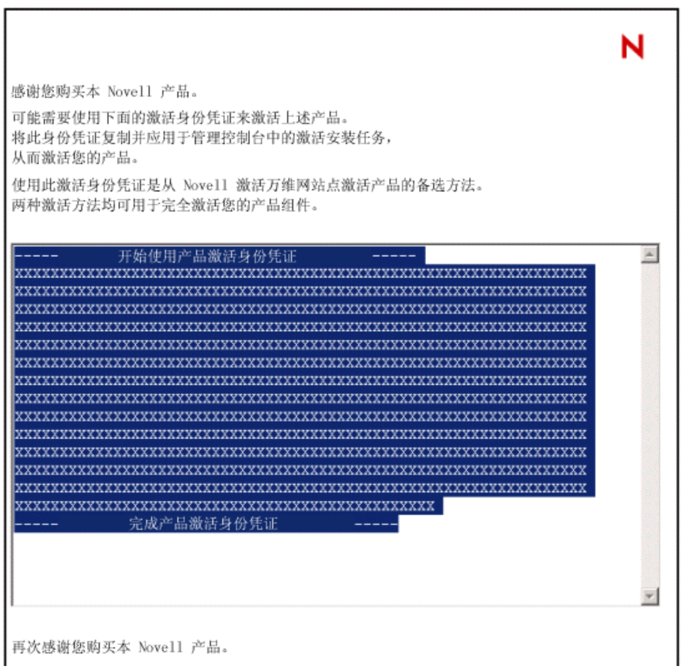
重要 : 激活产品不需要电子邮件。如果电子邮件被发送到您公司内得其他人那里，请联系 “Novell 激活中心”获取详细信息。

单击此链接后，将看到如下页面：



2 单击许可证下载链接，然后保存（下载）或打开 .html 文件。

文件打开后，其内容应类似于下图中显示的内容：



3 有关如何激活 Identity Manager 组件的指导，请继续第 6.3 节“安装产品激活身份凭证”（第 171 页）。

6.3 安装产品激活身份凭证

应该通过 iManager 安装产品激活身份凭证。

1 打开包含产品激活身份凭证的 Novell 电子邮件。

2 执行以下步骤之一：

- 保存产品激活身份凭证文件。

  或

- 打开产品激活身份凭证文件，然后将其内容复制到剪贴板。复制内容时要细心，确保没有包含额外的行或空格。应从身份凭证的第一个破折号 (-) 开始复制 (----BEGIN PRODUCT ACTIVATION CREDENTIAL)，一直复制到其最后一个破折号 (-) (END PRODUCT ACTIVATION CREDENTIAL-----)。

3 打开 iManager。

4 选择 *Identity Manager* > *Identity Manager 概述*。

5 选择驱动程序集，或浏览找到驱动程序集，然后单击 *下一步*。

6 在 "Identity Manager 概述" 页上，找到驱动程序集，单击红色的 *请求激活的用户*链接，然后单击 *安装激活*。

7 选择要激活 Identity Manager 组件的驱动程序集。

8 执行以下步骤之一：

- 指定 Identity Manager 激活身份凭证保存的位置，然后单击 *下一步*。

  或

- 将 Identity Manager 激活身份凭证的内容粘贴到文本区域，然后单击 *下一步*。

9 单击 *完成*。

注释 : 需要激活每个包含驱动程序的驱动程序集。可以使用身份凭证激活所有树。

6.4 查看 Identity Manager 和驱动程序的产品激活

对于每个驱动程序集，都可以看到为元目录引擎和 Identity Manager 驱动程序已安装的产品激活身份凭证。要查看产品激活身份凭证，请执行下列操作：

1. 打开 iManager。
2. 单击 *Identity Manager* > *Identity Manager 概述*。
3. 在对象名字段中，指定要查看其激活信息的驱动程序集或驱动程序的名称。

   或

   浏览并选择要查看其激活信息的驱动程序集或驱动程序。
4. 找到要查看其激活信息的驱动程序集，然后单击该驱动程序集的名称。
5. 选择*激活*选项卡。

   可以查看激活身份凭证的文本，或者，如果报告了错误，则可以去除激活身份凭证。

注释 : 为驱动程序集安装了有效的产品激活身份凭证后，驱动程序名的旁边可能仍然会显示 “要求激活”。如果出现这种情况，请重启动驱动程序，此后该讯息应会消失。
